Ranks of elliptic curves over function fields

Alan G.B. Lauder

February 2, 2008

Abstract

We present experimental evidence to support the widely held belief that one half of all elliptic curves have infinitely many rational points. The method used to gather this evidence is a refinement of an algorithm due to the author which is based upon rigid and crystalline cohomology.

1 Introduction

There is a widely held belief that one half of all elliptic curves have infinitely many rational points, but all experimental data which has been collected so far suggests that the fraction is actually two thirds [2, Introduction, Items (1) and (2)]. The final purpose of this paper is to present experimental evidence supporting the widely held belief. Let us first digress, to explain the origin of the method which has been used to collect this evidence.

In an earlier paper, the present author introduced a new method for computing zeta functions of varieties over finite fields [18]. The principal novelty of the method was that it proceeded by induction on the dimension of the variety. The author named it the *fibration method*. It was observed that the method appeared to be especially useful for the case of surfaces over finite fields which can be fibred into low genus curves. Given such a surface, the interesting part of its zeta function is exactly the L-function associated to the generic fibre — the generic fibre is a curve over a function field. According to a conjecture of Tate [23], the L-function reveals arithmetic properties of the curve, such as the rank of the group of rational points on its Jacobian. In the present paper, we carefully refine the fibration method, focussing ultimately on the case of elliptic curves over the rational function field, and use it to compute the L-functions of a randomly chosen sample of elliptic curves of extremely large conductor from a certain family. The computations reveal that around one half of those have rank, or at least analytic rank, greater than zero; see Section 9.

Leaving aside this final motivating application, the central achievement of this paper is the further development of the fibration method, with an emphasis upon the computation of L-functions of hyperelliptic curves over the rational function field. We shall now sketch the improvements to the method which are obtained. We need to introduce some notation: For q a power of a prime p, let $\mathbb{F}_q$ denote the finite field with q elements of characteristic p, K denote the unique unramified extension of the field of p-adic numbers of degree $\log_p(q)$, and W denote the ring of integers of K.

The challenge which we address is that of efficiently computing the zeta function of a smooth variety over a finite field $\mathbb{F}_q$. Our methods are based upon rigid and crystalline cohomology. Using standard techniques, one sees that the problem of central interest is that of calculating the pth power Frobenius action on the middle-dimensional rigid cohomology of the variety. This is a finite-dimensional vector space over K. In the case in which the original variety V of dimension n can be fibred into smooth varieties $V \to S$ over a curve $S \subset \mathbb{P}^1$, the paper [18] presents a method of reducing the problem of computing Frobenius on $H^n_{rig}(V)$ to that of computing Frobenius on $H^{n-1}_{rig}(V_0)$ for one smooth fibre $V_0 \hookrightarrow V$ in the family. So the method proceeds by induction on the dimension. We now describe how the work in this paper refines the fibration method.

First, the method requires that a basis be found for the relative cohomology space $H_{rig}^{n-1}(V/S)$ such that the "matrix for the Gauss-Manin connection is Fuchsian" [18, Section 4]. This is an entirely reasonable assumption as such bases are known to exist for families, for example, with an irreducible monodromy group, at least after extending the base field; however, the problem of actually finding such bases is an interesting open one, related to Hilbert's 21st problem. An exposition of this problem is given, and modest contributions made, in Sections 7 and 8.3; however, this still remains an obstacle to the wider application of the fibration method.

Second, in [18, Section 9.3] some new ideas on how to significantly improve the practical performance of the fibration method are sketched, although no details are offered. We work out these ideas in great detail and use them in our calculations for elliptic curves. Specifically, let X be some smooth compactification of the variety V. There is a finitely generated W-module $H_{cris}^n(X)$ attached to X called the middle-dimensional crystalline cohomology, and a natural map $H_{cris}^n(X) \to H_{rig}^n(V)$. The idea is that one computes a basis for the Frobenius-invariant W-lattice $H(X)_{prim} = \mathrm{Im}(H_{cris}^n(X) \to H_{rig}^n(V))$ and calculates Frobenius on this basis. Working with this basis, one can exploit the Hodge filtration to significantly reduce the p-adic precision to which the matrix for Frobenius needs to be computed. Rather than find $H(X)_{prim}$ itself, in Section 3 and 4 for certain surfaces X we describe how to compute a lattice $H(X, kD)$ (where D is a smooth divisor and k a suitably large integer) which is very close, in a precise sense, to $H(X)_{prim}$, although possibly of larger rank. This lattice is sufficient for our application and easier to find.

Third, in [18, Conjecture 7.4] a conjecture is made on the vanishing of certain coefficients in the "relative Frobenius matrix" attached to families $V \to S$ of hyperelliptic curves and a choice of basis for $H_{rig}^1(V/S)$. The truth of this conjecture immediately yields improvements to the running time of the original fibration method, see [18, Examples 9.2, 9.3], and also the refined method of this paper. We prove the conjecture. This also gives a practical improvement when one uses the deformation method to compute zeta functions of hyperelliptic curves over finite fields.

We now explain in greater detail the main theoretical contribution of this paper. Namely, our construction and application of W-lattices sitting in the middle-dimensional rigid cohomology of surfaces. This is the second refinement to the fibration method as introduced above.

For U a smooth surface of degree d in $\mathbb{A}_{\mathbb{F}_q}^3$, under certain assumptions for each $k \geq \max\{2d - 4, 0\}$ we explicitly construct a full rank W-lattice $H(X, kD)$ sitting in the K-vector space $H_{rig}^2(U)$. The motivation for constructing this lattice is Theorem 5.1. This theorem asserts that when $q = p$ is prime, if we compute an approximation $\tilde{A}$ to the matrix A for the pth power Frobenius map F with respect to a basis for this lattice, the loss of precision in the calculation of $\det(1 - p^{-1}\tilde{A}T)$ is bounded by $h^{2,0} + \lfloor \log_p(k+1) \rfloor$. Here $h^{2,0}$ is the geometric genus of a smooth compactification of a lifting to W of U. Using an arbitrary basis of $H_{rig}^2(U)$, even when $\tilde{A}$ has entries in W the author does not know how to improve the naive loss of precision bound of $\dim(H_{rig}^2(U)) - 1$ (or $\lfloor \dim(H_{rig}^2(U))/2 \rfloor - 1$ using the functional equation). For the surfaces we implicitly consider in Section 9, we have $p = 7$ and $(h^{2,0}, \dim(H_{rig}^2(U)), d) \in \{(0, 8, 6), (1, 20, 12), (2, 32, 18), (3, 44, 24), (4, 56, 30)\}$. So the use of a basis for $H(X, kD)$ makes a very significant impact on precisions required. Lying behind Theorem 5.1 is the existence of an embedding $H(X, \log D) \to H(X, kD)$ with cokernel killed by multiplication by $p^{\lfloor \log_p(k+1) \rfloor}$, where $H(X, \log D) \subset H_{rig}^2(U)$ is a full rank W-lattice endowed with what we call a Frobenius-Hodge structure (Definition 3.12). In the case in which U compactifies to a smooth surface X in $\mathbb{P}_{\mathbb{F}_q}^3$ with smooth divisor at infinity, then our lattice $H(X, \log D)$ is exactly the log-crystalline cohomology of the pair (X, D), where $D := X \backslash U$ (Section 3). Unfortunately, for the surfaces we are mainly interested in (Sections 8 and 9), this compactification is not smooth. The surfaces U we are mainly interested in do compactify to quasi-smooth surfaces X in weighted projective spaces. We make the additional assumption that these weighted projective surfaces are quotients of smooth surfaces $\tilde{X}$ in $\mathbb{P}_{\mathbb{F}_q}^3$ with smooth divisor at infinity $\tilde{D}$ under a natural finite group action. The lattices $H(X, \log D)$ and $H(X, kD)$ are then *defined* by taking the invariant part under this group action of the lattices $H(\tilde{X}, \log \tilde{D})$ and $H(\tilde{X}, k\tilde{D})$ associated to the affine part $\tilde{U} := \tilde{X} \backslash \tilde{D}$ of the smooth projective surface $\tilde{X}$ (Section 4.1). The lattices $H(X, \log D)$ and $H(X, kD)$ sit naturally in $H_{rig}^2(U)$, and we prove that $H(X, \log D)$ has a Frobenius-Hodge structure (Section

2

4.2). However, we stress that we do not prove that $H(X, \log D)$ is the log-crystalline cohomology of anything (although it undoubtedly is), see Note 4.8.

The second and third refinements to the fibration method do not impact in any dramatic manner on the asymptotic analysis of running time of the method; see Section 8.4 for a discussion. Their significance is perhaps best appreciated with reference to explicit examples. Regarding the second refinement, in [18, Example 9.1] a nine-fold speed-up is obtained by assuming the truth of [18, Conjecture 7.4]. Regarding the third refinement, in Section 9 the author computes, amongst other things, the L-functions of 1000 elliptic curves over $\mathbb{F}_7(t)$ which have discriminant a squarefree polynomial of degree 60. For each curve, the computation took around 1 hour using the second and third refinements in this paper (the first is not relevant for the curves chosen). With only the second refinement, each computation would have taken around 4 hours. We note that in our computations in Section 9, and the timing presented in this paragraph, we use an algorithm due to K. Kedlaya for recovering Weil polynomials from their p-adic approximations. [17, Section 4]. The output of our implementation of Kedlaya's algorithm is provably correct, although there are no explicit bounds on its running time. All of our calculations are done using the computer algebra system MAGMA.

We conclude the introduction with a brief mention of the contents of the other sections in this paper. Section 2 gives an overview of our refined fibration method and its relevance to the computation of L-functions. Section 6 proves some theorems of modest interest relating to one of the steps in the method, and includes a short discussion of the computation of the residue map.

2 The refined fibration method

The purpose of this section is to give an outline of the fibration method. The outline is based upon the original method presented in [18], incorporating refinements to the improvements crudely sketched in [18, Section 9.3]. To deal with the method in full would require the introduction of a great burden of notation, so we shall focus on aspects of it that are developed in this paper, and refer to [18] for details on parts which are fully investigated in that paper.

2.1 p-adic rings and finite fields

Let us first fix some notation which will be used throughout the paper. Let $\mathbb{F}_q$ be the finite field with q elements of characteristic p, $W := W(\mathbb{F}_q)$ be the ring of Witt vectors of $\mathbb{F}_q$, and K be the fraction field of W. Thus K is the unramified extension of the field of p-adic numbers of degree $\log_p(q)$, and W is the ring of integers of K. Let $\sigma : W \to W$ and $\sigma_K : K \to K$ be the Frobenius automorphisms on W and K respectively, that is, the maps induced by functoriality by the pth power map on $\mathbb{F}_q$. Let $\bar{\mathbb{F}}_q$ denote an algebraic closure of $\mathbb{F}_q$, and for each integer $k \geq 1$, let $\mathbb{F}_{q^k}$ denote the unique extension of degree k of $\mathbb{F}_q$ in $\bar{\mathbb{F}}_q$.

We warn the reader that the notation for the different varieties required in this paper is not consistent with that in [18]. The reason for this is that the focus of the two papers is quite different, and the notation from [18] would become burdensome in the present paper.

2.2 The zeta function and reduction to the middle dimension

Let X be a smooth projective variety of dimension n over the finite field $\mathbb{F}_q$ of characteristic p. The *zeta function* $Z(X, T)$ is the formal power series

$$Z(X, T) := \exp\left(\sum_{k=1}^{\infty} |X(\mathbb{F}_{q^k})| \frac{T^k}{k}\right)$$

which encodes the number of $\mathbb{F}_{q^k}$-rational points $|X(\mathbb{F}_{q^k})|$ on X over the different finite extensions $\mathbb{F}_{q^k}$ of the base field $\mathbb{F}_q$. By a famous theorem of Dwork, $Z(X,T)$ is a rational function. There is a formula from rigid cohomology [20, Pages 7-9]

$$Z(X,T) = \prod_{i=0}^{2n} \det(1 - Tq^n F_q^{-1} | H_{rig}^i(X))^{(-1)^{i+1}};$$

here each $H_{rig}^i(X)$ is a finite dimensional K-vector space, and F_q a linear map induced by the qth power map on the structure sheaf $\mathcal{O}_X$ of X. There is a factorisation $F_q = F^{\log_p(q)}$ where F is the σ_K-linear map on $H_{rig}^i(X)$ induced by the pth power map on $\mathcal{O}_X$.

The problem we consider is to compute $Z(X,T)$ given equations defining the variety X. We shall now try and convince the reader that the central problem is computing the factor with $i = n$.

First, we observe that if X is a hypersurface in a space whose zeta function is known, then by Poincaré duality and the Lefschetz hyperplane theorem, one can reduce immediately to the case $i = n$. So let us suppose we are not in such a fortunate situation. We shall proceed by induction on the dimension, and assume one can compute zeta functions of smooth zero dimensional varieties — we offer no suggestions on how this base case should be tackled. By Poincaré duality, one need only calculate the factors in the formula for $0 \le i \le n$. Let us assume that $X \subseteq \mathbb{P}^m$, and there exists a smooth hyperplane section $Y \hookrightarrow X$ defined over the finite field $\mathbb{F}_q$ — this is certainly the case after extending the base field. The Lefschetz hyperplane theorem then reveals that the factors for $0 \le i < n-1$ in the zeta function of $Z(Y,T)$ determine the corresponding factors in $Z(X,T)$. So by induction we reduce to the cases $i = n-1, n$. We suggest two different approaches to dealing with the case $i = n-1$. First, Deligne's pgcd theorem [6, Théorème 4.5.1] tells us that if one could compute the zeta functions of all smooth hyperplane sections in some Lefschetz pencil on X, then the $(n-1)$st factor could be recovered by computing a greatest common divisor. Unfortunately, the author is not aware of any effective bounds on how many hyperplane sections need to be considered until one recovers the correct polynomial; in practice, though, this would seem a useful approach. Second, a more sophisticated, but rigorous, method for obtaining the $(n-1)$st factor would be to use the spectral sequence in the fibration method, c.f. the proof of Proposition 6.1. This should not be too difficult, although the author does not offer any details. In any case, we hope the reader is convinced that the case $i = n$ is the one of main interest.

The problem on which we now focus is that of calculating a p-adic approximation to a matrix for F on the space $H_{rig}^n(X)$.

2.3 How the fibration method calculates in the middle dimension

2.3.1 The geometric set-up

Let $\mathcal{X}$ be a smooth W-scheme of relative dimension n and $\mathcal{D}$ a smooth divisor on $\mathcal{X}$. Assume that $\mathcal{U} := \mathcal{X} \backslash \mathcal{D}$ is affine, and embed it in some affine space $\mathbb{A}_W^m$, $m \ge n+1$. Choose a fibration $\mathbb{A}_W^m \to \mathbb{A}_W^1$. Let $\mathcal{U} \to \mathbb{A}_W^1$ be the restriction to $\mathcal{U}$. Choose $\mathcal{V} \subseteq \mathcal{U}$ so that the restriction $\mathcal{V} \to \mathcal{S} \subseteq \mathbb{A}_W^1$ has smooth fibres, and define $\mathcal{Z} := \mathcal{U} \backslash \mathcal{V}$. By varying the embedding we may assume $\mathcal{U} \to \mathbb{A}_W^1$ is generically smooth, and so $\mathcal{Z}$ is of codimension one. Let $\mathcal{V}_s$ for $s \in \mathcal{S}(W)$ be some smooth fibre in the family $\mathcal{V} \to \mathcal{S}$ — one may need to extend the base field $\mathbb{F}_q$ to find a smooth fibre. Let the special fibres and generic fibres of $\mathcal{X}, \mathcal{D}, \mathcal{U}, \mathcal{V}, \mathcal{Z}$ be denoted X, D, U, V, Z and $\mathcal{X}_K, \mathcal{D}_K, \mathcal{U}_K, \mathcal{V}_K, \mathcal{Z}_K$, respectively. Note that n is the dimension of the special fibre X. For example, if $\mathcal{X} \subset \mathbb{P}_W^m$ then one can construct a Lefschetz pencil on $\mathcal{X}_K$ with axis lying in the divisor $\mathcal{D}_K$. The singular fibres in $\mathcal{U}_K \to \mathcal{S}_K$ will each then only have unique double-points.

2.3.2 F-crystals and isocrystals

Definition 2.1. *An F-crystal is a finitely generated W-module M with a linear map $F : \sigma^* M \to M$ which becomes an isomorphism after tensoring with K. An F-isocrystal is a finite dimensional K-vector space V with a linear map $F : \sigma_K^* V \to V$ which is an isomorphism.*

4

That is, an F-crystal is a finitely generated W-module M with a σ-linear map $F : M \to M$ which becomes an injection after tensoring by K, and an F-isocrystal is a finite dimensional K-vector space with an injective σ_K-linear map $F : V \to V$. Define the F-crystal $W(m) \, (m \in \mathbb{Z}, \, m \leq 0)$ to be the rank one module over W where F acts on the basis elements by multiplication by p^{-m}, and likewise for $K(m) \, (m \in \mathbb{Z})$. We define Tate twists $M(m) := M \otimes_W W(m)$ of an F-crystal M, and likewise for F-isocrystals.

Let i be an integer. Associated to $\mathcal{X}$ and $\mathcal{D}$ are F-crystals

$$H^i_{cris}(X), H^i_{cris}(D), \text{ and } H^i_{cris}((X,D))$$

called the crystalline cohomology of X and D and log-crystalline cohomology of the pair (X,D), respectively. The groups above fit together in an F-equivariant long exact sequence [1, Definition 2.3.3, Proposition 2.4.1, Proposition 2.2.8]

$$\cdots \to H^i_{cris}(X) \to H^i_{cris}((X,D)) \to H^{i-1}_{cris}(D)(-1) \to \cdots \qquad (1)$$

Associated to $\mathcal{X}$, $\mathcal{D}$, $\mathcal{U}$, $\mathcal{V}$, Z and V_s are F-isocrystals

$$H^i_{rig}(X), \; H^i_{rig}(D), \; H^i_{rig}(U), \; H^i_{rig}(V), \text{ and } H^i_{rig}(V_s)$$

called the rigid cohomology of the special fibres, and F-isocrystals $H^i_{rig,Z}(U)$ called the rigid cohomology of U with support in Z. There is an F-equivariant long exact sequence

$$\cdots \to H^i_{rig,Z}(U) \to H^i_{rig}(U) \to H^i_{rig}(V) \to \cdots . \qquad (2)$$

(The F-isocrystals $H^i_{rig,Z}(U)$ are really just defined to make this sequence exact [16, Section 4.4].) There are natural maps

$$\begin{aligned} H^i_{cris}(X) & \to & H^i_{rig}(X) \\ H^i_{cris}((X,D)) & \to & H^i_{rig}(U) \end{aligned}$$

which are injections modulo torsion with images full rank W-lattices [1, Definition 2.3.3, Proposition 2.4.1]. We shall use the same symbol F to denote the Frobenius action on each of the F-crystals and F-isocrystals listed above.

Definition 2.2. *The following images are Frobenius-invariant W-lattices sitting naturally in K-vector spaces; that is, F-crystals embedded naturally in F-isocrystals.*

$$\begin{aligned} H(X)_{prim} & := & \mathrm{Im}(H^n_{cris}(X) \to H^n_{rig}(U)) \\ H(X, \log D) & := & \mathrm{Im}(H^n_{cris}((X,D)) \to H^n_{rig}(U)) \\ H(X) & := & \mathrm{Im}(H^n_{cris}(X) \to H^n_{rig}(X)). \end{aligned}$$

For the surfaces we consider, the lattice $H(X)_{prim}$ is exactly the free part of the primitive middle-dimensional crystalline cohomology.

2.3.3 A summary of the method

We wish to calculate a p-adic approximation to a matrix for the action of F on the full rank Frobenius-invariant W-lattice $H(X)$. The reason why it is important to work with a basis for this lattice rather than an arbitrary basis is given in [18, Section 9.3.2]. Essentially, one can exploit the Hodge filtration to significantly reduce the power of p to which the matrix needs to be calculated. We first note that it is both easier and more efficient to compute a matrix for F on the W-lattice $H(X)_{prim}$. It is easier because U is affine and so the elements in $H^n_{rig}(U)$ can be described via n-forms defined on $\mathcal{U}_K$. It is more efficient, at least for the case $n = 2$ of surfaces, since $H(X)_{prim}$ is the quotient of $H(X)$ by the rank one lattice generated by the class of the curve D, and the Frobenius action on the class of this curve is just multiplication by q.

The steps in our algorithm for calculating F on the lattice $H(X)_{prim}$ and our work upon the different steps can be tersely summarised as follows.

- STEP 1: Find a set of n-forms in $\Gamma(\mathcal{U}_K, \Omega^n_{\mathcal{U}_K})$ whose image in $H^n_{rig}(U)$ is a basis for the full rank W-lattice $H(X, \log D)$. [This is the problem of finding explicit bases in log-crystalline cohomology. It is solved for surfaces in certain weighted projective spaces in Sections 3 and 4.]

- STEP 2: Use the long exact sequence for crystalline and log-crystalline cohomology (1) to compute a basis for the sublattice $H(X)_{prim} \subseteq H(X, \log D)$ from one for $H(X, \log D)$ itself. [This is the problem of explicitly computing the residue map. It is briefly discussed in Section 6.3.]

- STEP 3: Use the long exact sequence in rigid cohomology (2) to map the basis elements for $H(X)_{prim}$ into the space $H^n_{rig}(V)$. Thus one reduces the problem to that of calculating the action of F on the space $H^n_{rig}(V)$. [We discuss this in Section 6 for certain surfaces.]

- STEP 4: Use the smooth fibration $V \to S$ to reduce the problem to that of calculating the action of F on the space $H^{n-1}_{rig}(V_s)$ for one smooth fibre $V_s \hookrightarrow V$ defined over $\mathbb{F}_q$. [This is the heart of the fibration method, and is dealt with in detail in [18, Sections 3, 4, 5]. One outstanding problem which is not fully resolved in [18] is that of finding a Fuchsian basis. This problem is explained in Section 7, and in Section 8.3 a solution for elliptic curves is given using an algorithm due to W. Dekkers.]

In practice, it is not always necessary or desirable to carry out Steps 1 and 2 exactly as stated. First, it is easier though perhaps slightly less efficient to compute a matrix for F on the full W-lattice $H(X, \log D)$ rather than its sublattice $H(X)_{prim}$; that is, to omit Step 2. Second, it is not necessary to find $H(X, \log D)$ exactly, as a lattice which is very close to it will be sufficient. For example, in our application to surfaces X we actually work with a lattice $H(X, kD)$ ($k \gg 0$, see Theorem 3.11 and Definition 4.9) such that

$$H(X)_{prim} \overset{i}{\hookrightarrow} H(X, \log D) \overset{\rho}{\hookrightarrow} H(X, kD) \subseteq H^2_{rig}(U)$$

where the cokernel of the embedding ρ is killed by $p^{\lfloor \log_p(k+1) \rfloor}$. For certain elliptic surfaces the map i is an isomorphism and when p is large enough relative to the degree of the surface so is ρ, so we find $H(X)_{prim}$ exactly. For the examples we present in Section 9, the corank of the image of i is 2, and the map ρ has cokernel killed by at worst p^2. So $H(X, kD)$ contains a sublattice of corank 2 which is very close to $H(X)_{prim}$. This is good enough for our application. Theorem 5.1 exactly quantifies the benefits one obtains from working with a basis of the lattice $H(X, kD)$.

2.4 L-functions

We now explain the relevance of our algorithm to the computation of L-functions of certain curves. Let $U \subset \mathbb{A}^3_{\mathbb{F}_q}$ be a smooth affine surface and $U \to \mathbb{A}^1_{\mathbb{F}_q}$ be the fibration via one of the coordinate axes. Assume that one can extend $U \to \mathbb{A}^1_{\mathbb{F}_q}$ to a map $\hat{X} \to \mathbb{P}^1_{\mathbb{F}_q}$ where $\hat{X}$ is a smooth projective surface. Assume that the singular fibres of the map are geometrically irreducible, so the trivial part of the Néron-Severi lattice of $\hat{X}$ is generated by the class of the zero section and a smooth fibre. Define the F-invariant W-lattice

$$H := \mathrm{Image}(H^2_{cris}(\hat{X}) \to H^2_{rig}(U)).$$

We shall define the L-function of the generic curve $\hat{X}_\eta$ in the family $\hat{X} \to \mathbb{P}^1_{\mathbb{F}_q}$ to be

$$L(\hat{X}_\eta, T) := \det(1 - TF_q | H \otimes_W K).$$

This agrees with the usual definition, since it is exactly the "interesting part" of the zeta function, obtained from $P_2(\hat{X}, T) := \det(1 - TF_q | H^2_{rig}(\hat{X}))$ by removing factors coming from the classes of the zero section and a smooth fibre in $H^2_{cris}(\hat{X})$.

Note that in our application we shall compactify U to a (quasi-smooth) surface X in weighted projective space, and the lattice $H(X)_{prim}$ will then be defined (see Section 4.2) and equal to H above.

3 Crystalline cohomology of smooth surfaces in $\mathbb{P}^3$

In this section we address the problem of finding the lattice $H(X, \log D) = \mathrm{Im}(H^n_{cris}((X, D)) \to H^n_{rig}(U))$, in the case in which X is a smooth surface of degree d sitting in projective space $\mathbb{P}^3_{\mathbb{F}_q}$. We shall proceed in some generality in Sections 3.1, 3.2 and 3.3, before specialising to smooth surfaces in $\mathbb{P}^3_{\mathbb{F}_q}$ in Section 3.4. Ultimately, we will be satisfied with finding a lattice $H(X, kD)$, for any $k \geq \max\{2d - 4, 0\}$, which contains $H(X, \log D)$ as a sublattice, with the quotient an abelian group killed by multiplication by $p^{\lfloor \log_p(k+1) \rfloor}$. We use these lattices to define analogous lattices in Section 4 associated to certain weighted projective surfaces, and explain why all of these lattices are useful in Section 5.

3.1 Crystalline and de Rham cohomology

Let $\mathcal{X}$ be a smooth W-scheme of relative dimension 2 and $\mathcal{D}$ a smooth divisor on $\mathcal{X}$. For $i \geq 0$, denote by $\Omega^i_{\mathcal{X}} := \wedge^i \Omega^1_{\mathcal{X}}$ the sheaf of differential i-forms on $\mathcal{X}$, and by

$$\Omega^\bullet_{\mathcal{X}} : 0 \to \mathcal{O}_{\mathcal{X}} \to \Omega_{\mathcal{X}} \to \Omega^2_{\mathcal{X}} \to 0$$

the algebraic de Rham complex of $\mathcal{X}$. The algebraic de Rham cohomology $H_{dR}(\mathcal{X})$ of $\mathcal{X}$ is by definition the hypercohomology $\mathbb{H}(\Omega^\bullet_{\mathcal{X}})$ of this complex. This is a finitely generated W-module. The complex $\Omega^\bullet_{\mathcal{D}}$ and finitely generated W-module $H_{dR}(\mathcal{D}) := \mathbb{H}(\Omega^\bullet_{\mathcal{D}})$ are defined in an analogous manner. For $i \geq 0$, denote by $\Omega^i(\log \mathcal{D}) := \wedge^i \Omega^1_{\mathcal{X}}(\log \mathcal{D})$ the sheaf of differential i-forms on X with logarithmic poles along $\mathcal{D}$, and by

$$\Omega^\bullet_{\mathcal{X}}(\log \mathcal{D}) : 0 \to \mathcal{O}_{\mathcal{X}} \to \Omega_{\mathcal{X}}(\log \mathcal{D}) \to \Omega^2_{\mathcal{X}}(\log \mathcal{D}) \to 0$$

the logarithmic de Rham complex [1, Definition 2.2.2]. The log-de Rham cohomology $H_{dR}((\mathcal{X}, \mathcal{D}))$ is by definition the hypercohomology $\mathbb{H}(\Omega^\bullet_{\mathcal{X}}(\log \mathcal{D}))$ of this complex. This is a finitely generated W-module. There is an exact sequence

$$0 \to \Omega^\bullet_{\mathcal{X}} \to \Omega^\bullet_{\mathcal{X}}(\log \mathcal{D}) \stackrel{Res}{\to} j_* \Omega^\bullet_{\mathcal{D}}[+1] \to 0$$

where the map Res is the residue map and $j : \mathcal{D} \hookrightarrow \mathcal{X}$ [1, Proposition 2.2.8]. This induces a long exact sequence on the hypercohomology groups:

$$\cdots \to H^i_{dR}(\mathcal{X}) \to H^i_{dR}((\mathcal{X}, \mathcal{D})) \to H^{i-1}_{dR}(\mathcal{D}) \to \cdots .$$

Let X and D be the special fibres of $\mathcal{X}$ and $\mathcal{D}$ respectively. Associated to the smooth pair of $\mathbb{F}_q$-varieties (X, D) are finitely generated W-modules with canonical isomorphisms [1, Definition 2.3.3, Proposition 2.4.1]

$$H_{cris}(X) \cong H_{dR}(\mathcal{X}), \ H_{cris}(D) \cong H_{dR}(\mathcal{D}), \ H_{cris}((X, D)) \cong H_{dR}((\mathcal{X}, \mathcal{D})).$$

These are the crystalline and log-crystalline cohomology groups. The aim of this section is to give an explicit presentation of the log-crystalline cohomology groups $H^i_{cris}((X, D))$ in terms of the homology of a complex of free W-modules of finite rank.

3.2 The hypercohomology of the logarithmic de Rham complex

For $i, k \geq 0$, let $\Omega^i(k\mathcal{D}) := \Omega^i_{\mathcal{X}} \otimes_{\mathcal{O}_{\mathcal{X}}} \mathcal{O}_{\mathcal{X}}(k\mathcal{D})$ denote the sheaf of differential i-forms on $\mathcal{X}$ with poles of order bounded by k along $\mathcal{D}$. Consider the complex

$$\Omega^\bullet_{\mathcal{X}}((k + \bullet)\mathcal{D}) : 0 \to \mathcal{O}_{\mathcal{X}}(k\mathcal{D}) \to \Omega_{\mathcal{X}}((k+1)\mathcal{D}) \to \Omega^2_{\mathcal{X}}((k+2)\mathcal{D}) \to 0.$$

Theorem 3.1. *The cokernels of the maps of homology sheaves induced by the natural map of complexes of sheaves*

$$\Omega^\bullet_{\mathcal{X}}(\log \mathcal{D}) \hookrightarrow \Omega^\bullet_{\mathcal{X}}((k + \bullet)\mathcal{D})$$

are killed by multiplication by $\mathrm{lcm}\{1, 2, \ldots, k + 1\}$. Moreover, the induced maps on homology sheaves are injective.

Proof. We will show using étale local coordinates that for each $0 \le i \le 2$ the map of homology sheaves
$$\mathcal{H}^i(\Omega_{\mathcal{X}}^\bullet(\log \mathcal{D})) \to \mathcal{H}^i(\Omega_{\mathcal{X}}^\bullet((k + \bullet)\mathcal{D}))$$
is an injection and has cokernel killed by $\operatorname{lcm}\{1, 2, \ldots, k+i-1\}$. We shall use subscripts x and y to denote partial differentiation w.r.t. x and y, respectively.

For points not lying on $\mathcal{D}$ there is nothing to prove, since locally at these points the sheaves are isomorphic. Etale locally around a point on $\mathcal{D}$ the pair $(\mathcal{X}, \mathcal{D})$ looks like the hyperplane section $x = 0$ of an open subset $\operatorname{Spec}(R)$ of $\operatorname{Spec}(W[x, y])$. By a further Zariski localisation we may assume R contains a subring isomorphic to $R/(x)$, and derivation w.r.t. x is trivial on this subring. (That is, with $S := \{y_0 \mid (0, y_0) \not\in \operatorname{Spec}(R)\}$, replace R by $R' := R[1/(y - y_0); y_0 \in S]$ and then $W[y][1/(y-y_0); y_0 \in S]$ is the required subring of R' isomorphic to $R'/(x)$; then replace the notation R' by R.) Let ℓ be a positive integer, and define $n_\ell := \operatorname{lcm}\{1, 2, \ldots, \ell - 1\}$. For $a = \sum_{i=-\ell}^{-1} a_i(y)x^i \in R[x^{-1}]$ where $a_i(y) \in R/(x) \subset R$, define $\hat{a} := \sum_{i=-\ell}^{-2}(a_i(y)/(i+1))x^{i+1} \in R[x^{-1}] \otimes_W K$. Then $\hat{a}_x = a + (a_{-1}(y)/x)$ and $n_\ell \hat{a} \in R[x^{-1}]$.

For $i = 0$ there is nothing to prove since the closed 0-forms are just the constant functions for both sheaves. For $i = 2$, let $\alpha(x, y)dx \wedge dy \in \Omega_{R[x^{-1}]}^2$ be a closed 2-form with a pole of order $k+2$. Let $\alpha = a(x, y) + b(x, y)$ where b has no pole along $\mathcal{D}$, and write a as in the preceding paragraph, taking $\ell = k + 2$. Define $\beta := \hat{a}dy \in \Omega_{R[x^{-1}]}^1 \otimes_W K$. Then $\alpha dx \wedge dy - d\beta = \frac{a_{-1}dx}{x} \wedge dy + \gamma$ where the 2-form γ has no pole along $\mathcal{D}$. Morever, $n_{k+2}\beta \in \Omega_{R[x^{-1}]}$. Thus after multiplication by n_{k+2} locally any 2-form can be written modulo exact 2-forms as a 2-form with a log-pole along $\mathcal{D}$. This proves the claim on the cokernel for $i = 2$.

We now consider the cokernel for $i = 1$. Let $\alpha = \beta(x, y)dx + \gamma(x, y)dy \in \Omega_{R[x^{-1}]}^1$ be a closed 1-form with a pole of order $k + 1$ along $\mathcal{D}$. Since α is closed, $\beta_y = -\gamma_x$. As before, write $\beta = a(x, y) + b(x, y)$ where b has no pole along $\mathcal{D}$, and write a as above, taking $\ell = k + 1$. Then $\alpha - d(\hat{a}) = \frac{a_{-1}dx}{x} + (\gamma - \hat{a}_y)dy$. Using the equation $\beta_y = -\gamma_x$ we see that $\gamma - \hat{a}_y$ has no pole along $\mathcal{D}$. Thus after multiplication by n_{k+1} locally any closed 1-form can be written modulo exact 1-forms as a 1-form with a log-pole along $\mathcal{D}$.

We now prove the maps on sheaves are injective by examining kernels. For $i = 0$ there is nothing to prove. For $i = 1$, a closed 1-form $\alpha \in \Omega_{R[x^{-1}]}^1$ with a log-pole has the form $\beta(x, y)\frac{dx}{x} + \gamma(x, y)dy$ where the functions $\beta, \gamma \in R$ have no poles along $\mathcal{D}$, with $(\beta/x)_y = -\gamma_x$. Suppose that $\alpha = df$ for some function $f(x, y) \in R[x^{-1}]$ with a pole of order $\ell \ge 1$ along $\mathcal{D}$. Since $f_y = \gamma$, we see f_y has no pole along $\mathcal{D}$, so f must be independent of y with $\gamma = f_y = 0$. Thus $(\beta/x)_y = 0$, so β does not depend on y, and we have $f(x)_x = \beta(x)/x$. This can only be true if $\beta(x)/x$ has no pole along $\mathcal{D}$, and so neither does f, a contradiction. Thus no such f can exist, and the map on homology sheaves is injective for $i = 1$.

Now let $i = 2$. A (closed) 2-form $\alpha \in \Omega_{R[x^{-1}]}^2$ with a log-pole locally has the form $\beta(x, y)\frac{dx}{x} \wedge dy$ for some function $\beta \in R$ with no pole along $\mathcal{D}$. Suppose that $\alpha = d\gamma$ where the 1-form $\gamma \in \Omega_{R[x^{-1}]}^1$ has a pole of order $\ell \ge 1$ along $\mathcal{D}$. We shall show that the exists a 1-form $\gamma' \in \Omega_{R[x^{-1}]}^1$ with a log-pole along $\mathcal{D}$ such that $\alpha = d\gamma'$. This proves our map of homology sheaves is injective on 2-forms.

Write $\gamma = a(x, y)dx + b(x, y)dy$. Let $a = a'' + a'$ and $b = b'' + b'$ where a' has a simple pole along $\mathcal{D}$ with $a'' := a - a' = \sum_{i=-\ell}^{-2} a_i(y)x^i$, and b' has no pole along $\mathcal{D}$ with $b'' := b - b' = \sum_{i=-\ell}^{-1} b_i(y)x^i$. Then since $\beta(x, y)/x = b_x - a_y$ has a log-pole, we see $b_{-\ell} = 0$, and for $i = -\ell, -\ell + 1, \ldots, -2$ we have $(a_i)_y = (i + 1)b_{i+1}$. Hence $\gamma'' := a''dx + b''dy$ is a closed 1-form. Defining $\gamma' := a'dx + b'dy$ one sees that γ' has a log-pole along $\mathcal{D}$. Moreover, $\alpha = d\gamma = d(\gamma' + \gamma'') = d\gamma'$, as required. $\square$

Note 3.2 An analogue of the claim on the cokernel is proved in [1, Theorem 2.2.5] with the complex $\Omega_{\mathcal{X}}^\bullet((k + \bullet)\mathcal{D})$ replaced by the twisted logarithmic complex whose ith term is $\Omega_{\mathcal{X}}^i(\log \mathcal{D}) \otimes_{\mathcal{O}_{\mathcal{X}}} \mathcal{O}_{\mathcal{X}}(k\mathcal{D})$, for the more general situation in which $\mathcal{D}$ is a smooth normal crossings divisor in a smooth W-scheme $\mathcal{X}$ of arbitrary dimension n.

Define the complex of sheaves $Q^\bullet$ on $\mathcal{X}$ so that the sequence
$$0 \to \Omega_{\mathcal{X}}^\bullet(\log \mathcal{D}) \to \Omega_{\mathcal{X}}^\bullet((k + \bullet)\mathcal{D}) \to Q^\bullet \to 0 \tag{3}$$

is exact.

Corollary 3.3. *The homology sheaves $\mathcal{H}^i(Q^\bullet)$ of the complex $Q^\bullet$ are killed by multiplication by $\mathrm{lcm}\{1, 2, \ldots, k+1\}$.*

Proof. The long exact sequence for homology sheaves from the short exact sequence (3) has the form

$$\cdots \to \mathcal{H}^i(\Omega_{\mathcal{X}}^\bullet(\log \mathcal{D})) \xrightarrow{\theta_i} \mathcal{H}^i(\Omega_{\mathcal{X}}^\bullet((k+\bullet)\mathcal{D})) \xrightarrow{\phi_i} \mathcal{H}^i(Q^\bullet)$$

$$\xrightarrow{\psi_i} \mathcal{H}^{i+1}(\Omega_{\mathcal{X}}^\bullet(\log \mathcal{D})) \xrightarrow{\theta_{i+1}} \mathcal{H}^i(\Omega_{\mathcal{X}}^\bullet((k+\bullet)\mathcal{D})) \xrightarrow{\phi_{i+1}} \cdots$$

Since θ_{i+1} is an injection by Theorem 3.1, $\mathcal{H}^i(Q^\bullet)$ is isomorphic to the cokernel of θ_i and thus by that theorem is killed as claimed. □

In the nicest situation one has the following corollary to Theorem 3.1.

Corollary 3.4. *If the characteristic p of the residue field of W is strictly greater than $k+1$, then we have the following isomorphism of hypercohomology groups:*

$$H_{dR}((\mathcal{X}, \mathcal{D})) := \mathbb{H}(\Omega_{\mathcal{X}}^\bullet(\log \mathcal{D})) \cong \mathbb{H}(\Omega_{\mathcal{X}}^\bullet((k+\bullet)\mathcal{D})).$$

Proof. Since in this case $\mathrm{lcm}\{1, 2, \ldots, k+1\}$ is invertible in W, for each i by Theorem 3.1 we have an isomorphism of homology sheaves $\mathcal{H}^i(\Omega_{\mathcal{X}}^\bullet(\log \mathcal{D})) \cong \mathcal{H}^i(\Omega_{\mathcal{X}}^\bullet((k+\bullet)\mathcal{D}))$. These homology sheaves are the first terms in a spectral sequence $E_2^{p,q} := H^p(\mathcal{X}, \mathcal{H}^p(\star))$ computing the hypercohomology of each complex of sheaves $\star$ [9, Remark 2.1.6 (i)]. Hence the hypercohomology groups are isomorphic. □

In general, one must be satisfied with the next corollary.

Corollary 3.5. *Let $\mathbb{H}^i$ denote the ith hypercohomology group. The kernel and cokernel of the map $\mathbb{H}^i(\Omega_{\mathcal{X}}^\bullet(\log \mathcal{D})) \to \mathbb{H}^i(\Omega_{\mathcal{X}}^\bullet((k+\bullet)\mathcal{D}))$ are killed by multiplication by $p^{\lfloor \log_p(k+1) \rfloor}$.*

Proof. In this case by Corollary 3.4 for each i the homology sheaves $\mathcal{H}^i(Q^\bullet)$ are killed by multiplication by $p^{\lfloor \log_p(k+1) \rfloor}$ and hence so is the hypercohomology $\mathbb{H}(Q^\bullet)$. The result follows from the long exact sequence in hypercohomology for the short exact sequence (3). □

3.3 The hypercohomology of $\Omega_{\mathcal{X}}^\bullet((k+\bullet)\mathcal{D})$.

The hypercohomology of $\Omega_{\mathcal{X}}^\bullet((k+\bullet)\mathcal{D})$ is accessible because of the following proposition.

Proposition 3.6. *Assume $k \geq 0$ is chosen so that the sheaves $\Omega_{\mathcal{X}}^i((k+i)\mathcal{D})$ are acyclic for $i = 0, 1, 2$. Then the hypercohomology of $\Omega_{\mathcal{X}}^\bullet((k+\bullet)\mathcal{D})$ is canonically isomorphic to the homology of the complex $\Gamma(\mathcal{X}, \Omega_{\mathcal{X}}^\bullet((k+\bullet)\mathcal{D}))$ of rings of global sections:*

$$0 \to \Gamma(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(k\mathcal{D})) \to \Gamma(\mathcal{X}, \Omega_{\mathcal{X}}((k+1)\mathcal{D})) \xrightarrow{d} \Gamma(\mathcal{X}, \Omega_{\mathcal{X}}^2((k+2)\mathcal{D})) \to 0.$$

Proof. The hypercohomology of $\Omega_{\mathcal{X}}^\bullet((k+\bullet)\mathcal{D})$ may be calculated via a spectral sequence, the first terms of which are the W-modules $E_1^{p,q} := H^q(\mathcal{X}, \Omega_{\mathcal{X}}^p((k+p)\mathcal{D}))$ [9, Remark 2.1.6 (ii)]. Since the sheaves are acyclic, $E_1^{p,q} = 0$ for $q > 0$, and so this spectral sequence degenerates after the first term. Hence the hypercohomology is just the homology of the complex of rings of global sections. □

Corollary 3.7. *Assume that $k \geq 0$ is chosen to satisfy the conditions of Proposition 3.6. Then the natural map*

$$H_{cris}^2((X, D)) \to \frac{\Gamma(\mathcal{X}, \Omega_{\mathcal{X}}^2((k+2)\mathcal{D}))}{d(\Gamma(\mathcal{X}, \Omega_{\mathcal{X}}^1((k+1)\mathcal{D}))} \tag{4}$$

has kernel and cokernel killed by multiplication by $p^{\lfloor \log_p(k+1) \rfloor}$. In particular, for $p > k+1$ this map is an isomorphism.

Proof. This follows from Corollary 3.5 and Proposition 3.6 and the natural isomorphism $H_{dR}^\bullet((\mathcal{X}, \mathcal{D})) \cong H_{cris}^\bullet((X, D))$. □

By Serre's vanishing theorem [11, Theorem III.5.2.(b)], the hypothesis of Proposition 3.6 will be satisfied for $k \gg 0$. It remains to calculate an explicit value for k that one may choose. We shall do this for the case in which $\mathcal{X}$ is a smooth surface in $\mathbb{P}^3$.

Note 3.8 The twisted logarithmic de Rham complex whose ith term is $\Omega^i_{\mathcal{X}}(\log \mathcal{D}) \otimes_{\mathcal{O}_{\mathcal{X}}} \mathcal{O}_{\mathcal{X}}(k\mathcal{D})$, which appears in [1, Theorem 2.2.5], will also be acyclic for $k \gg 0$. However, the complex $\Omega^\bullet_{\mathcal{X}}((k + \bullet)\mathcal{D})$ seems easier to compute with.

3.4 Vanishing theorems for smooth surfaces in $\mathbb{P}^3$

In this section we calculate explicit values of k which make the sheaves $\Omega^i_{\mathcal{X}}((k + i)\mathcal{D})$ acyclic, for $\mathcal{X}$ a smooth surface in $\mathbb{P}^3_W$.

Let $\mathcal{X}$ be a smooth surface of degree d in projective space $\mathbb{P} := \mathbb{P}^3_W$ with ideal sheaf $I \cong \mathcal{O}_{\mathbb{P}}(-d)$. The latter condition is satisfied precisely when the surface $\mathcal{X} \otimes_W \mathbb{F}_q$ is of degree d. For $k \in \mathbb{Z}$ let $\mathcal{O}_{\mathcal{X}}(k)$ denote the twisting sheaf, and as usual define $\Omega^i_{\mathcal{X}}(k) := \Omega^i_{\mathcal{X}} \otimes_{\mathcal{O}_{\mathcal{X}}} \mathcal{O}_{\mathcal{X}}(k)$. Let $\mathcal{D}$ be a hyperplane section. For any $k \in \mathbb{Z}$ we have $\Omega^i_{\mathcal{X}}(k\mathcal{D}) := \Omega^i_{\mathcal{X}} \otimes_{\mathcal{O}_{\mathcal{X}}} \mathcal{O}_{\mathcal{X}}(k\mathcal{D}) \cong \Omega^i_{\mathcal{X}}(k)$.

The proof of the following theorem was explained to the author by Bjorn Poonen.

Theorem 3.9 (Poonen). *The sheaves $\mathcal{O}_{\mathcal{X}}(k), \Omega_{\mathcal{X}}(k)$ and $\Omega^2_{\mathcal{X}}(k)$ are acyclic for $k > d - 4$, $k > \max\{2d - 4, 0\}$, and $k > 0$, respectively.*

Proof. Let F be the defining polynomial for the surface $\mathcal{X}$, and $\pi : \mathcal{X} \hookrightarrow \mathbb{P}$. The proof is based upon the following three exact sequences of sheaves c.f. [11, II.8.17, II.8.13]

$$0 \to \mathcal{O}_{\mathbb{P}}(-d) \xrightarrow{\times F} \mathcal{O}_{\mathbb{P}} \to \pi_* \mathcal{O}_{\mathcal{X}} \to 0 \text{ on } \mathbb{P}. \tag{5}$$

$$0 \to I/I^2 \to \Omega_{\mathbb{P}}|_{\mathcal{X}} \to \Omega_{\mathcal{X}} \to 0 \text{ on } \mathcal{X} \tag{6}$$

$$0 \to \Omega_{\mathbb{P}} \to \mathcal{O}_{\mathcal{X}}(-1)^{\oplus 4} \to \mathcal{O}_{\mathbb{P}} \to 0 \text{ on } \mathbb{P}, \tag{7}$$

and the calculation of the homology of projective 3-space $\mathbb{P}$ c.f. [11, III.5]

$$\begin{aligned} &H^0(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(e)) = 0 \text{ for } e < 0 \\ &H^1(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(e)) = H^2(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(e)) = 0 \text{ for all } e \\ &H^3(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(e)) = 0 \text{ for } e > -4. \end{aligned}$$

Since $\mathcal{O}_{\mathbb{P}}(e)$ is locally free and hence flat we may twist (5) by $\mathcal{O}_{\mathbb{P}}(e)$ and take homology to obtain the exact sequences

$$H^i(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(e)) \to H^i(\mathbb{P}, \pi_* \mathcal{O}_{\mathcal{X}}(e)) \to H^{i+1}(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(e - d)) \text{ for } i \geq 0. \tag{8}$$

Since π is affine, we have $H^i(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(e)) \cong H^i(\mathbb{P}, \pi_* \mathcal{O}_{\mathcal{X}}(e))$ and from (8) and the homology of $\mathbb{P}$ we see that the latter vanishes for $i > 0$ and $e - d > -4$.

Next, restricting (7) to $\mathcal{X}$, twisting by $\mathcal{O}_{\mathcal{X}}(e)$ and taking homology we get exact sequences

$$H^{i-1}(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(e)) \to H^i(\mathcal{X}, \Omega_{\mathbb{P}}(e)|_{\mathcal{X}}) \to H^i(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(e - 1))^{\oplus 4} \text{ for } i \geq 1.$$

Using our result on the vanishing of $H^i(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(e))$ we immediately deduce

$$H^i(\mathcal{X}, \Omega_{\mathbb{P}}(e)|_{\mathcal{X}}) = 0 \text{ for } i > 1 \text{ and } e > d - 3.$$

For $i = 1$, we need also determine when the the map

$$H^0(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(e - 1))^{\oplus 4} \to H^0(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(e)) \tag{9}$$

is a surjection. We need to determine explicitly what the spaces are and map is. First, twisting (5) by $\mathcal{O}_{\mathbb{P}}(e)$ and using the fact $H^1(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(e)) = 0$ we get that $H^0(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(e))$ equals the quotient of the space of homogeneous polynomials of degree e modulo those of the form FG where G is homogeneous of degree $e - d$. Second, observe that the map in (9) comes from that in (7), and the ith component is just multiplication by the ith variable X_i. So the map is surjective as soon

10

as $e > 0$; for one can obtain any monomial of degree $e > 0$ by multiplying some monomial of degree $e - 1$ by one of the X_i. Thus the map is surjective when $e > 0$, and so $H^1(\mathcal{X}, \Omega_{\mathbb{P}}(e)|_{\mathcal{X}}) = 0$ for $e > \max\{0, d - 3\}$.

Now observe since $I \cong \mathcal{O}_{\mathbb{P}}(-d)$ we have

$$I/I^2 \cong I \otimes \mathcal{O}_{\mathbb{P}}/I \cong \mathcal{O}_{\mathbb{P}}(-d) \otimes \mathcal{O}_{\mathcal{X}} = \mathcal{O}_{\mathcal{X}}(-d).$$

So twisting (6) by $\mathcal{O}_{\mathcal{X}}(e)$ and taking homology we get exact sequences

$$H^i(\mathcal{X}, \Omega_{\mathbb{P}}(e)|_{\mathcal{X}}) \to H^i(\mathcal{X}, \Omega_{\mathcal{X}}(e)) \to H^{i+1}(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(e - d)) \text{ for } i \geq 0.$$

Thus $H^i(\mathcal{X}, \Omega_{\mathcal{X}}(e)) = 0$ for $i > 0$ and $e > \max\{0, 2d - 4\}$.

Finally, taking top exterior powers in (6) one deduces $\Omega_{\mathcal{X}}^2 \cong \mathcal{O}_{\mathcal{X}}(d - 4)$, which completes the proof. $\square$

3.5 Crystalline lattices for smooth surfaces in $\mathbb{P}^3$

The next two theorems are the main results of Section 3.

Theorem 3.10. *Let X be a smooth surface in $\mathbb{P}_W^3$ of degree d which remains of degree d when reduced modulo p, and D the hyperplane section at infinity which we assume to be smooth. Let $k + 1 > \max\{2d - 4, 0\}$. Then the natural map*

$$H^2_{cris}((X, D)) \to \frac{\Gamma(\mathcal{X}, \Omega_{\mathcal{X}}^2((k+2)\mathcal{D}))}{d(\Gamma(\mathcal{X}, \Omega_{\mathcal{X}}^1((k+1)\mathcal{D})))} \tag{10}$$

has kernel and cokernel killed by multiplication by $p^{\lfloor \log_p(k+1) \rfloor}$.

Proof. Immediate from Corollary 3.7 and Theorem 3.9 $\square$

Theorem 3.11. *With notation as in Theorem 3.10, let $H(X, kD)$ denote the image of the righthand side of (10) in $H^2_{rig}(U)$, where $U = X \backslash D$. Let $H(X, \log D)$ denote the image of $H^2_{cris}((X, D))$ in $H^2_{rig}(U)$. Then there is a natural embedding $H(X, \log D) \to H(X, kD)$ with cokernel killed by multiplication by $p^{\lfloor \log_p(k+1) \rfloor}$.*

Proof. The maps $H^2_{cris}((X, D)) \to H(X, \log D)$ and

$$\frac{\Gamma(\mathcal{X}, \Omega_{\mathcal{X}}^2((k+2)\mathcal{D}))}{d(\Gamma(\mathcal{X}, \Omega_{\mathcal{X}}^1((k+1)\mathcal{D})))} \to H(X, kD)$$

are isomorphisms modulo torsion. The map $H(X, \log D) \to H(X, kD)$ is defined via these isomorphisms, and its cokernel is killed as claimed by Theorem 3.10. It is am embedding since the kernel of the map (10) is torsion. $\square$

3.6 Frobenius-Hodge structures for smooth surfaces in $\mathbb{P}^3$

In this section we gather some results which will be applied in Sections 4.2 and 5. We begin with an entirely utilitarian definition whose relevance will shortly become apparent. Note that it is exactly adequate for our purposes but inadequate for general use.

Definition 3.12. *A torsion-free F-crystal H has a (pure) Frobenius-Hodge structure if there exists $j, m \in \mathbb{Z}$ with $j, m \geq 0$ and a filtration by submodules $0 = H_{m+1} \subseteq H_m \subseteq \cdots \subseteq H_0 = H$ such that $F(H_i) \subseteq p^{j+i}(H)$ for $0 \leq i \leq m$. A torsion-free F-crystal H has a (mixed) Frobenius-Hodge structure if there exists a short exact sequence of F-crystals $0 \to H_1 \to H \to H_2 \to 0$ such that H_1 and H_2 have pure Frobenius-Hodge structures.*

Let $\mathcal{X}$ be a smooth hypersurface in $\mathbb{P}_W^n$ with special fibre X and generic fibre $\mathcal{X}_K$. Then the W-modules $H^j(\mathcal{X}, \Omega_{\mathcal{X}}^i)$ are torsion free [21, Page 660, Lines 15-16], and thus so are $H^m_{cris}(X)$ (this is implied by the remarks [21, Page 662, Lines 7-9] and the statement of [21, Theorem

11

2]). We define the Hodge numbers $h^{i,j} := \operatorname{rank}(H^j(\mathcal{X}, \Omega^i_{\mathcal{X}})) = \dim(H^j(\mathcal{X}_K, \Omega^i_{\mathcal{X}_K}))$. Note that $h^{i,j} = h^{j,i}$. Let p be the residue characteristic of W, and assume that $p > n - 1 = \dim(X)$. The following result is from [21, Section 5]. There exist a filtration (Hodge filtration)

$$0 := H_{m+1,m} \subseteq H_{m,m} \subseteq H_{m-1,m} \subseteq \cdots \subseteq H_{0,m} = H^m_{cris}(X)$$

such that the pth power Frobenius F acts as $F(H_{i,m}) \subseteq p^i H^m_{cris}(X)$. Moreover, $\operatorname{rank}(H_{i,m}/H_{i+1,m}) = h^{i,m-i}$ for $0 \le i \le m$. Thus $H^m_{cris}(X)$ has a pure Frobenius-Hodge structure, see Definition 3.12, with the ranks of the submodules in the filtration determined by the Hodge numbers of $\mathcal{X}_K$.

Now let $\mathcal{X}$ be a smooth surface in $\mathbb{P}^3_W$. Let $\mathcal{D} \subset \mathbb{P}^2_W$ be the curve at infinity, which we assume to be smooth. Then the results in the above paragraph apply to give pure Frobenius-Hodge structures on $H^2_{cris}(\mathcal{X})$ and $H^1_{cris}(\mathcal{D})$. Since $H^1_{cris}(X) = H^3_{cris}(X)$ are torsion-free, and we know $H^1_{rig}(X) = H^3_{rig}(X) = 0$, by the Lefschetz hyperplane theorem, one deduces $H^1_{cris}(X) = H^3_{cris}(X) = 0$. Moreover, since the cycle class map is injective in codimension 1 [23, Page 97], from (14) one deduces the following exact sequence.

$$0 \to W(-1) \to H^2_{cris}(X) \to H^2_{cris}((X, D)) \to H^1_{cris}(D)(-1) \to 0. \tag{11}$$

Note that F acts by multiplication by p on the rank 1 F-crystal $W(-1)$, so $H^2_{cris}(X)/W(-1)$ has a pure Frobenius-Hodge structure. The sequence (11) shows that $H^2_{cris}((X, D))$ is torsion-free, and defines a mixed Frobenius-Hodge structure on $H^2_{cris}((X, D))$, see Definition 3.12

4 Weighted projective surfaces

In this section we consider the case in which $\mathcal{X}$ is a surface of degree d in the weighted projective space $\mathbb{P}(1, a, b, c)_W$. Following a suggestion of A.J. de Jong, we view $\mathcal{X}$ in a standard way as the quotient of a surface $\tilde{\mathcal{X}}$ in $\mathbb{P}^3$ by the action of a finite group $G \cong \mathbb{Z}/(a) \times \mathbb{Z}/(b) \times \mathbb{Z}/(c)$. We assume that $\tilde{\mathcal{X}}$ is smooth with the G-invariant divisor at infinity $\tilde{\mathcal{D}}$ smooth, and also that the affine piece $\mathcal{U} := \mathcal{X} \cap \mathbb{A}^3_W$ is smooth. Under these assumptions, we define a lattice $H(X, \log D) \subset H^2_{rig}(U)$ and for each $k \ge \max\{2d - 4, 0\}$ explicitly construct a lattice $H(X, kD) \subset H^2_{rig}(U)$ such that there is a embedding $H(X, \log D) \to H(X, kD)$ with cokernel killed by multiplication by $p^{\lfloor \log_q(k+1) \rfloor}$. We explain the importance of the lattices $H(X, \log D)$ and $H(X, kD)$ in Section 5.

4.1 The lattices $H(X, \log D) \subseteq H(X, kD)$ in $H^2_{rig}(U)$

We first define our ambient weighted projective space.

Definition 4.1. *Let a, b, c be positive integers, and $\mathbb{P}(1, a, b, c)_W$ be a weighted projective space over W; that is, $\operatorname{Proj}(S)$ where the ring $S := W[T, X, Y, Z]$ is graded by assigning weights $\operatorname{wt}(T) := 1, \operatorname{wt}(X) := a, \operatorname{wt}(Y) := b, \operatorname{wt}(Z) := c$. Assume that the residue characteristic p of W does not divide abc.*

Note that if desired one can assume that $\gcd(a, b, c) = 1$ (although this plays no part in our proofs) since in any case $\mathbb{P}(1, a, b, c)_W \cong \mathbb{P}(1, a/e, b/e, c/e)_W$ where $e := \gcd(a, b, c)$ [7, Page 186].

The open subscheme defined by $T \ne 0$ is isomorphic to affine 3-space $\mathbb{A}^3_W$ with coordinates given by $x := X/T^a, y := Y/T^b$ and $z := Z/T^c$. Let $R := W[X_0, X_1, X_2, X_3]$ be the graded polynomial ring with $\operatorname{wt}(X_i) := 1$ for $0 \le i \le 3$ and define projective 3-space $\mathbb{P}^3_W := \operatorname{Proj}(R)$. Consider the injective map of graded rings

$$\pi : S \to R, \ T \mapsto X_0, \ X \mapsto X_1^a, \ Y \mapsto X_2^b, \ Z \mapsto X_3^c.$$

This induces a quotient map $\mathbb{P}^3_W \to \mathbb{P}(1, a, b, c)_W$ of topological spaces.

Assume now that W is large enough to contain primitive ath, bth and cth roots of unity ζ_a, ζ_b and ζ_c, respectively. See Note 4.11 for a discussion of the general case. Let the group $G := \mathbb{Z}/(a) \times \mathbb{Z}/(b) \times \mathbb{Z}/(c)$ act on R by

$$G \times R \to R, \ (i, j, k) \times f(X_0, X_1, X_2, X_3) \mapsto f(X_0, \zeta_a^i X_1, \zeta_b^j X_2, \zeta_c^k X_3).$$

Lemma 4.2. *The invariant subring R^G of R under the action of G is exactly $\pi(S) = R[X_0, X_1^a, X_2^b, X_3^c]$.*

Proof. Certainly $\pi(S) \subseteq R^G$. Suppose now that $f = \sum_i a_i X^i \in R^G$ where $i := (i_0, i_1, i_2, i_3) \in \mathbb{Z}_{\geq 0}^4$ and $X^i := X_0^{i_0} \cdots X_3^{i_3}$. Since G acts on each term $a_i X^i$ in f by scalar multiplication, each term in f must be fixed by G. So it is enough to consider the case of a single monomial $f = X_0^{i_0} \cdots X_3^{i_3}$. By considering the action of $(1,0,0), (0,1,0), (0,0,1) \in G$ in turn, one deduces that $a|i_1, b|i_2$ and $c|i_3$, so $f \in \pi(S)$, as required. $\qquad\square$

Corollary 4.3. *The weighted projective space $\mathbb{P}(1, a, b, c)_W$ is isomorphic to the quotient scheme $\mathbb{P}_W^3/G$.*

Proof. By Lemma 4.2, $S \overset{\pi}{\cong} R^G$, and so $\operatorname{Proj}(S) \cong \operatorname{Proj}(R^G) =: \mathbb{P}_W^3/G$. $\qquad\square$

Let $\mathcal{X}$ be a hypersurface in $\mathbb{P}(1, a, b, c)_W$ defined by a weighted homogeneous polynomial $P(T, X, Y, Z)$ of degree d. Assume that the hypersurface $\tilde{\mathcal{X}}$ in $\mathbb{P}_W^3$ defined by the polynomial $\pi(P) = P(X_0, X_1^a, X_2^b, X_3^c)$ is a smooth W-scheme with ideal sheaf $I \cong \mathcal{O}_{\mathbb{P}_W^3}(-d)$. Define $\mathcal{D}$ and $\tilde{\mathcal{D}}$ to be the divisors on $\mathcal{X}$ and $\tilde{\mathcal{X}}$, respectively, defined by the ideals (T) and (X_0), respectively. Let $\mathcal{U} := \mathcal{X} \backslash \mathcal{D}$ and $\tilde{\mathcal{U}} := \tilde{\mathcal{X}} \backslash \tilde{\mathcal{D}}$.

Lemma 4.4. *The group G acts on $\tilde{\mathcal{X}}$ with $\mathcal{X} \cong \tilde{\mathcal{X}}/G$, on $\tilde{\mathcal{U}}$ with $\mathcal{U} \cong \tilde{\mathcal{U}}/G$, and on $\tilde{\mathcal{D}}$ with $\mathcal{D} \cong \tilde{\mathcal{D}}/G$.*

Proof. The group G acts on $\tilde{\mathcal{X}}$ since the ideal $(\pi(P))$ is G-invariant. Now $\tilde{\mathcal{X}}/G := \operatorname{Proj}((R/(\pi(P)))^G)$ and we note $(R/(\pi(P)))^G \cong R^G/(\pi(P))$. The isomorphism $S \overset{\pi}{\to} R^G$ reduces modulo the homogeneous ideal (P) to an isomorphism $S/(P) \overset{\pi}{\to} R^G/(\pi(P)) = (R/(\pi(P)))^G$. So $\mathcal{X} = \operatorname{Proj}(S/(P)) = \tilde{\mathcal{X}}/G$.

Since G acts trivially on T, it acts on $\mathcal{U}$ with $(i, j, k) \times g(x, y, z) \mapsto g(\zeta_a^i x, \zeta_b^j y, \zeta_c^k z)$, for $g \in W[x, y, z] = W[X/T^a, Y/T^b, Z/T^c]$. The proof that $\mathcal{U} \cong \tilde{\mathcal{U}}/G$ is similar to that in the preceding paragraph. The group G acts on $\tilde{\mathcal{D}}$ since it fixes the homogeneous ideal (T), and one sees as before that $\mathcal{D} \cong \tilde{\mathcal{D}}/G$. $\qquad\square$

Let $X, D, U, \tilde{X}, \tilde{D}, \tilde{U}$ denote the special fibres. Assume that $\mathcal{U}$ is smooth.

Lemma 4.5. *For each $i \geq 0$, the group G acts on the rigid cohomology space $H_{rig}^i(\tilde{U})$ and $H_{rig}^i(U) \cong H_{rig}^i(\tilde{U})^G$.*

Proof. Let A and B denote the coordinate rings of $\mathcal{U}$ and $\tilde{\mathcal{U}}$, respectively; so $A \cong B^G$. Taking weak completions we have $A^\dagger \cong (B^G)^\dagger \cong (B^\dagger)^G$, the latter isomorphism follows since the action of G commutes with taking weak completions. Let $d : B^\dagger \to \Omega_{B^\dagger}$ be the universal derivation which is continuous w.r.t the p-adic metric on $B^\dagger$. One checks that $(\Omega_{B^\dagger}^\bullet)^G$ is the direct factor in $\Omega_{B^\dagger}^\bullet$ corresponding to the trivial character in a character-based decomposition, that $(\Omega_{B^\dagger}^\bullet)^G \cong \Omega_{(B^\dagger)^G}^\bullet$ as complexes of $(B^\dagger)^G$-modules, and since $(B^\dagger)^G \cong A^\dagger$ we have $\Omega_{(B^\dagger)^G}^\bullet \cong \Omega_{A^\dagger}^\bullet$. The rigid cohomology of $\tilde{U}$ is by definition the homology $H(\Omega_{B^\dagger}^\bullet)$. Since $(\Omega_{B^\dagger}^\bullet)^G$ is the trivial-character direct factor in $\Omega_{B^\dagger}^\bullet$ one has $H(\Omega_{B^\dagger}^\bullet)^G \cong H((\Omega_{B^\dagger}^\bullet)^G)$, and we know $H((\Omega_{B^\dagger}^\bullet)^G) \cong H(\Omega_{A^\dagger}^\bullet)$. But the latter is by definition the rigid cohomology of U. $\qquad\square$

Assume that $\tilde{\mathcal{D}}$ is a smooth divisor. Then the crystalline cohomology groups $H_{cris}^i((\tilde{X}, \tilde{D}))$ are defined, and there is a natural map

$$H_{cris}^i((\tilde{X}, \tilde{D})) \to H_{rig}^i(\tilde{U})$$

which is an injection modulo torsion with image a full-rank W-lattice. These morphisms commute with the action of G, so we may take G-invariants to get natural maps

$$H_{cris}^i((\tilde{X}, \tilde{D}))^G \to H_{rig}^i(\tilde{U})^G$$

and by Lemma 4.5 the image is isomorphic to $H_{rig}^i(U)$.

Definition 4.6. *For each $i \geq 0$, define the W-module $H^i_{cris}((X, D))$ to be the G-invariant part $H^i_{cris}((\tilde{X}, \tilde{D}))^G$. We shall call these groups the log-crystalline cohomology of the pair (X, D).*

Proposition 4.7. *There is a natural map which is an injection modulo torsion $H^i_{cris}((X, D)) \to H^i_{rig}(U)$, with image a full-rank F-invariant W-lattice. Let us denote this lattice $H(X, \log D)$.*

Proof. We constructed the natural map immediately before Definition 4.6, and it is an injection modulo torsion. It is F-invariant since the action of G commutes with the pth power map on the homogeneous coordinate ring $R/(\pi(P), p)$ of $\tilde{X}$. Since the order of G is coprime to p, there is a G-invariant decomposition

$$H^i_{cris}((\tilde{X}, \tilde{D})) = H^i_{cris}((\tilde{X}, \tilde{D}))^G \oplus C_{cris} \to H^i_{rig}(\tilde{U})^G \oplus C_{rig} = H^i_{rig}(\tilde{U})$$

and a natural map which is an injection modulo torsion $C_{cris} \to C_{rig}$. If the map in the proposition did not have a full-rank image, then the rank of the image of C_{cris} in C_{rig} would have to exceed the dimension of C_{rig}; an impossibility. $\square$

Note 4.8 The W-scheme $\mathcal{X}$ in general will only be quasi-smooth, that is have quotient singularities, which in our case lie along the divisor $\mathcal{D}$ [8, Appendix B]. So the log-crystalline cohomology $H^i_{cris}((X, D))$ is not a priori defined. The divisor $\mathcal{D}$ itself is a quasi-smooth curve in weighted projective space $\mathbb{P}(a, b, c)_W$. Quasi-smooth varieties are normal, and hence the curve $\mathcal{D}$ itself is smooth. The author believes that $H^2_{cris}((X, D))$ defined above is isomorphic to $H^2_{cris}((X_1, D_1))$ where X_1 is some smooth compactification of U with $D_1 := X_1 \backslash U_1$ a smooth normal crossing divisor; however, he offers no proof of this.

Using Theorem 3.10, the group $H^2_{cris}((\tilde{X}, \tilde{D}))$ can be explicitly described as the cohomology classes in $H^2_{rig}(\tilde{U})$ of a set of elements in $\Gamma(\tilde{\mathcal{U}}, \Omega^2_{\tilde{\mathcal{U}}})$. The G-invariants of this set are easily calculated. Explicitly, for $k + 1 > \max\{2d - 4, 0\}$ we see that the map

$$H^2_{cris}((X, D)) := H^2_{cris}((\tilde{X}, \tilde{D}))^G \to \frac{\Gamma(\tilde{\mathcal{X}}, \Omega^2_{\tilde{\mathcal{X}}}((k+2)\tilde{\mathcal{D}}))^G}{d(\Gamma(\tilde{\mathcal{X}}, \Omega^1_{\tilde{\mathcal{X}}}((k+1)\tilde{\mathcal{D}})))^G} = \frac{\Gamma(\mathcal{X}, \Omega^2_{\mathcal{X}}((k+2)\mathcal{D}))}{d(\Gamma(\mathcal{X}, \Omega^1_{\mathcal{X}}((k+1)\mathcal{D})))} \quad (12)$$

has kernel and cokernel killed by multiplication by $p^{\lfloor \log_p(k+1) \rfloor}$. The last equality of W-modules in (12) follows from the isomorphism $\Gamma(\mathcal{U}, \Omega^i_{\mathcal{U}}) \cong \Gamma(\mathcal{U}, (\rho_*\Omega^i_{\tilde{\mathcal{U}}})^G)$ where $\rho : \tilde{\mathcal{U}} \to \mathcal{U}$ is the quotient map, c.f. [22, Page 215, Lines 8-12], and the fact that pole orders are just calculated by taking suitable weighted degrees.

Definition 4.9. *For each $k + 1 \geq \max\{2d - 4, 0\}$, the lattice $H(X, kD)$ is defined to be the image of the righthand side of (12) in $H^2_{rig}(U)$.*

Proposition 4.10. *There is a natural embedding $H(X, \log D) \to H(X, kD)$ with cokernel killed by multiplication by $p^{\lfloor \log_p(k+1) \rfloor}$.*

Proof. Elements in the kernel of the natural map (12) must be torsion (take G-invariants in Corollary 3.5 applied to the pair $(\tilde{X}, \tilde{D})$) and so vanish in $H(X, \log D) = \mathrm{Im}(H^2_{cris}((X, D)) \to H^2_{rig}(U))$. The map in proposition is thus the embedding defined by pulling back elements in $H(X, \log D)$ to the free part of $H^2_{cris}((X, D))$, mapping via (12), and then embedding in $H^2_{rig}(U)$. $\square$

The K-vector space $H(X, kD) \otimes_W K$ is F-invariant and so has the structure of an F-isocrystal; however, $H(X, kD)$ itself is not in general F-invariant.

Note 4.11 Only the construction of the lattice $H(X, \log D)$ relies upon the existence of appropriate primitive roots $\zeta_a, \zeta_b, \zeta_c \in W^*$. The definition of $H(X, kD)$ does not, and indeed this lattice is independent of the choice of base field — see Section 4.3 for an example of how to construct this lattice. In the general case, one constructs a basis for the lattice $H(X, kD)$. The theory guarantees that if one extends the base field $\mathbb{F}_q$ to contain appropriate primitive roots, then this lattice is close to $H(X, \log D)$, and so is acted upon in a particular way by the

14

pth power Frobenius map F, see Section 5. But the action of the pth power Frobenius map is independent of the field over which the basis is defined, so it acts in that manner on the original lattice $H(X, kD) \subset H^2_{rig}(U)$.

Note 4.12 A direct application of Poonen's method to surfaces in weighted projective space and experiments suggest that in fact $k + 1 > \max\{2d - (1 + a + b + c), 0\}$ is sufficient for the map in (12) to have kernel and cokernel killed as claimed.

4.2 Frobenius-Hodge structures for weight projective surfaces

We continue with the notation and assumptions in Section 4.1. We shall also use the notation in the final paragraph of Section 3.6, only we now denote our smooth projective surface and curve as $\tilde{\mathcal{X}}$ and $\tilde{\mathcal{D}}$, respectively. Taking G-invariants in the exact sequence (11) for the pair $(\tilde{X}, \tilde{D})$ and noting the first non-zero term is $H^0_{cris}(\tilde{D})$ we get the sequence

$$0 \to W(-1) \to H^2_{cris}(\tilde{X})^G \to H^2_{cris}((X, D)) \to H^1_{cris}(\tilde{D})(-1)^G \to 0.$$

Since Frobenius F commutes with the action of G, the above exact sequence defines a mixed Frobenius-Hodge structure (Definition 3.12) on $H^2_{cris}((X, D))$. We examine this in more detail next.

Let us first recall how one defines Hodge numbers of quasi-smooth varieties, c.f. [4, Appendix A.3].

Definition 4.13. *Let $j : \mathcal{X}^s_K \to \mathcal{X}_K$ be the embedding of the smooth locus and $i \geq 0$, and define the sheaf $\hat{\Omega}^i_{\mathcal{X}_K} := j_* \Omega^i_{\mathcal{X}^s_K}$ on $\mathcal{X}_K$. The Hodge numbers $h^{i,j}$ are the dimensions of the K-vector spaces $H^j(\mathcal{X}_K, \hat{\Omega}^i_{\mathcal{X}_K})$.*

Note that $\mathcal{D}_K$ is smooth so its Hodge numbers are defined in the usual manner, as the dimensions of the spaces $H^j(\mathcal{D}_K, \Omega^i_{\mathcal{D}_K})$. By the result on [22, Page 215, Lines 8-12], for each $i \geq 0$ we have an isomorphism of sheaves $(\rho_* \Omega^i_{\tilde{\mathcal{D}}_K})^G \cong \Omega^i_{\mathcal{D}_K}$ and $(\rho_* \Omega^i_{\tilde{\mathcal{X}}_K})^G \cong \hat{\Omega}^i_{\mathcal{X}_K}$ where $\rho : \tilde{\mathcal{X}}_K \to \mathcal{X}_K$ is the quotient map and also its restriction $\rho : \tilde{\mathcal{D}}_K \to \mathcal{D}_K$. It follows by decomposing sheaves via characters of G and using the finiteness of ρ that $H^j(\tilde{\mathcal{X}}_K, \Omega^i_{\tilde{\mathcal{X}}_K})^G \cong H^j(\mathcal{X}_K, \hat{\Omega}^i_{\mathcal{X}_K})$ and $H^j(\tilde{\mathcal{D}}_K, \Omega^i_{\tilde{\mathcal{D}}_K})^G \cong H^j(\mathcal{D}_K, \Omega^i_{\mathcal{D}_K})$. Thus the dimensions of the graded pieces in the filtrations on $H^2_{cris}(\tilde{X})^G$ and $H^1_{cris}(\tilde{D})^G$ are just the Hodge numbers of the quasi-smooth surface $\mathcal{X}_K$ and smooth curve $\mathcal{D}_K$.

Since $H^2_{cris}((X, D))$ is a submodule of $H^2_{cris}((\tilde{X}, \tilde{D}))$ and the latter is torsion free, so is the former. Thus the lattice $H(X, \log D) := \mathrm{Im}(H^2_{cris}((X, D)) \to H^2_{rig}(U))$ is isomorphic to $H^2_{cris}((X, D))$. Defining $H(X)_{prim} := H^2_{cris}(X)^G / W(-1)$ we see that there is a filtration $0 \subseteq H_2 \subseteq H_1 \subseteq H_0 = H(X)_{prim}$ with $F(H_i) \subseteq p^i H(X)_{prim}$. Recall $h^{i,j} := \dim(H^j(\mathcal{X}_K, \hat{\Omega}^i_{\mathcal{X}_K}))$ are the Hodge numbers of the quasi-smooth variety $\mathcal{X}_K$. We have $h^{2,0} = \mathrm{rank}\, H_2$ and $h^{1,1} - 1 = \mathrm{rank}\,(H_1/H_2)$ (we have removed the hyperplane class), and $h^{0,2} = \mathrm{rank}\,(H_0/H_1)$. Defining $h_2 := h^{2,0} + h^{1,1} + h^{0,2}$, the middle Betti number of $\mathcal{X}_K$, we see that $H(X)_{prim}$ has rank $h_2 - 1$.

Likewise, the lattice
$$H(D) := \mathrm{Im}(H^1_{cris}(\tilde{D})^G \to H^1_{rig}(\tilde{D})^G)$$

is isomorphic to $H^1_{cris}(\tilde{D})^G$ and has a filtration $0 \subseteq H'_1 \subseteq H'_0 = H(D)$ with $F(H'_i) \subseteq p^i(H(D))$ and $\mathrm{rank}\, H'_1 = g = \mathrm{rank}\,(H'_0/H'_1)$ where $g := \dim(H^0(\mathcal{D}_K, \Omega^1_{\mathcal{D}_K}))$. So the mixed Frobenius-Hodge structure on $H(X, \log D) \cong H^2_{cris}((X, D))$ comes from the exact sequence

$$0 \to H(X)_{prim} \to H(X, \log D) \to H(D)(-1) \to 0$$

and the dimensions of the various graded pieces can be calculated from the Hodge numbers of the quasi-smooth surface $\mathcal{X}_K$ and smooth curve $\mathcal{D}_K$.

4.3 Surfaces of the form $z^2 = Q(x, y)$

We now describe an explicit method for constructing the lattice $H(X, kD)$ in the case in which $\mathcal{U}$ is a surface defined by a polynomial $z^2 = Q(x, y)$.

4.3.1 Differential forms on the surface

Assume that the characteristic p of the residue field of W is odd. Let a, b, c be positive integers with $\gcd(a, b) = 1$ and abc not divisible by p. Let $Q(x, y) = \sum_{i,j} q_{i,j} x^i y^j$ be a polynomial in $W[x, y]$ such that $ai + bj \le 2c$ for all pairs (i, j), with this bound met for some choice of pair (i, j); that is, $Q(x, y)$ has weighted degree $2c$ when one assigns weights $\mathrm{wt}(x) := a$ and $\mathrm{wt}(y) := b$ in the polynomial ring $W[x, y]$. Let $\mathcal{X}$ be the hypersurface of degree $d := 2c$ in $\mathbb{P}(1, a, b, c)_W$ defined by the polynomial

$$P := T^d \left((Z/T^c)^2 - Q(X/T^a, Y/T^b) \right).$$

Let $\mathcal{D}$ denote the scheme defined by the ideal (P, X_0) and $\mathcal{U} := \mathcal{X} \backslash \mathcal{D}$. The affine W-scheme $\mathcal{U}$ is defined by the polynomial $z^2 = Q(x, y)$, where $x = X/T^a, y = Y/T^b$ and $z := Z/T^c$. We assume that $\mathcal{U}$ is smooth. We further assume that the schemes $\tilde{\mathcal{X}}$ and $\tilde{\mathcal{D}}$, respectively, in $\mathbb{P}_W^3$ defined by the polynomial $\pi(P) := P(X_0, X_1^a, X_2^b, X_3^c)$ and ideal $(\pi(P), X_0)$, respectively, are smooth W-schemes, although this will play no role in the construction of the lattice $H(X, kD)$.

Lemma 4.14. *The functions $x, y,$ and z have poles of orders a, b and c, respectively, along the divisor $\mathcal{D}$. The 1-forms dx, dy and dz have poles of orders $a + 1, b + 1$ and $c + 1$ along $\mathcal{D}$, and the 2-form $dx \wedge dy$ a pole of order $a + b + 2$ along $\mathcal{D}$.*

Proof. Follows since the divisor $\mathcal{D}$ is defined by the homogeneous ideal (T), differentiation increases pole orders by one, and $dx \wedge dy = d(y dx)$. $\square$

By definition, the module $\Gamma(\mathcal{U}, \Omega_{\mathcal{U}}^1)$ is generated over $W[x, y, z]/(z^2 - Q(x, y))$ by the 1-forms dx, dy and dz subject to the one relation

$$2z dz = Q_x dx + Q_y dy.$$

It follows immediately that the module $\Gamma(\mathcal{U}, \Omega_{\mathcal{U}}^2)$ is generated over $W[x, y, z]/(z^2 - Q(x, y))$ by the 2-forms $dx \wedge dy, dy \wedge dz$ and $dz \wedge dx$ subject to the relations

$$dy \wedge dz = -\frac{Q_x}{2z} dx \wedge dy, \quad dz \wedge dx = -\frac{Q_y}{2z} dx \wedge dy.$$

Since $\mathcal{U}$ is smooth we have $(Q, Q_x, Q_y) = (1)$. A simple computation now reveals that

$$\Gamma(\mathcal{U}, \Omega_{\mathcal{U}}^2) = \left\{ \frac{A + Bz}{z} dx \wedge dy \mid A, B \in W[x, y] \right\}.$$

By Lemma 4.14, the pole order of such a 2-form along $\mathcal{D}$ is bounded above by

$$\max\{\mathrm{wt}(A) - c, \mathrm{wt}(B)\} + a + b + 2$$

where wt here means weighted degree.

Lemma 4.15. *Let $B \in W[x, y]$ have ordinary degree $\deg(B)$. Then for any $k + 2 \ge \mathrm{wt}(B) + a + b + 2$, the class of the 2-form $B dx \wedge dy$ in the quotient on the righthand side of (12) is killed by multiplication by $p^{\lfloor \log_p (\deg(B)) \rfloor}$; thus it is the zero class in $H_{rig}^2(U)$.*

Proof. Integrating w.r.t. x, say, one constructs a polynomial $C \in W[x, y]$ with $dC/dx = p^{\lfloor \log_p (\deg(B)) \rfloor} B$. Then $d(C \wedge dy) = p^{\lfloor \log_p (\deg(B)) \rfloor} B dx \wedge dy$, as required. $\square$

Since we wish to construct the image in $H_{rig}^2(U)$ of the righthand side of (12), by Lemma 4.15 we can restrict attention to 2-forms $(A/z) dx \wedge dy$.

By an explicit computation one finds that the exact forms $(A/z)dx \wedge dy$ are precisely those for which

$$2A = \alpha Q_x + \beta Q_y + 2(\alpha_x + \beta_y)Q, \ \alpha, \beta \in W[x,y].$$

Precisely, such a form is d of

$$Czdx + Dzdy + Edz, \ \alpha := D - E_y, \ \beta := -C + E_x, \ C, D, E \in W[x,y].$$

Note that the pole order of such a 1-form is bounded by $\max\{\mathrm{wt}(\alpha)+c+b+1, \mathrm{wt}(\beta)+c+a+1\}$. So to ensure this has pole order at most $k+1$ we need to have $\mathrm{wt}(\alpha) \leq (k+1)-(c+b+1) = k-(b+c)$ and $\mathrm{wt}(\beta) \leq k - (a+c)$. Moreover, the 2-forms $(A/z)dx \wedge dy$ have pole order bounded by $\mathrm{wt}(A) - c + a + b + 2$, so to ensure the pole order is at most $k+2$ it is enough to have $\mathrm{wt}(A) \leq (k+2) + c - (a+b+2) = k+c-(a+b)$.

4.3.2 An algorithm for constructing the lattice $H(X, kD)$

For any $k \geq 0$, one constructs a set which generates the quotient in (12) as follows. For any integer $m \geq 0$, let $\mathrm{Mon}_{\leq m}$ denote the union of the set of monomials $x^i y^j$ of weighted degree at most m with $\{0\}$. Let Z_m denote the free W-submodule of $W[x,y]$ spanned by the monomials in $\mathrm{Mon}_{\leq m+c-(a+b+2)}$. Let $B_m \subseteq Z_m$ be the W-module generated by polynomials of the form $\alpha Q_x + \beta Q_y + 2(\alpha_x + \beta_y)$ where $\alpha \in \mathrm{Mon}_{\leq(m-1)-(b+c+1)}$ and $\beta \in \mathrm{Mon}_{\leq(m-1)-(a+c+1)}$. Define $H_m := Z_m/B_m$. Then H_{k+2} is isomorphic to the quotient in (12) via the map

$$\theta : Z_{k+2} \to \Gamma(\mathcal{X}, \Omega^2_{\mathcal{X}}((k+2)\mathcal{D})), \ x^i y^j \mapsto x^i y^j dx \wedge dy/2z.$$

One can find a set $S(k) \subseteq \mathrm{Mon}_{\leq k+c-(a+b)}$ of monomials whose classes in H_{k+2} are a W-generating set for this quotient using the following method.

Let $Z_{m,p} := Z_m \otimes_W \mathbb{F}_q$ and $B_{m,p} := B_m \otimes_W \mathbb{F}_q$ be $\mathbb{F}_q$-vector spaces. Using linear algebra over $\mathbb{F}_q$, compute a generating set $S(k)$ of monomials for the quotient $Z_{k+2,p}/B_{k+2,p}$. Let $\langle S(k)\rangle_W$ denote the W-span of this generating set. Let $w \in Z_{k+2}$. Then $w = u_1 + v_1 \mod p$ for some $u_1 \in \langle S(k)\rangle_W$ and $v_1 \in B_{k+2}$. Write $w = u_1 + v_1 + pw_2$ where $w_2 \in Z_{k+2}$. Repeating the process we find $u_2 \in \langle S(k)\rangle_W$ and $v_2 \in B_{k+2}$ such that $w = (u_1 + pu_2) + (v_1 + pv_2) + p^2 w_2$ for some $w_2 \in Z_{k+2}$. By induction, and taking a p-adic limit, we find $u \in \langle S(k)\rangle_W$ and $v \in B_{k+2}$ such that $w = u + v$, as required.

If $p > k + 1$ and $k \geq \max\{2d - 4, 0\}$, and the classes of the forms

$$\theta(s) = (s/2z)dx \wedge dy \text{ for } s \in S(k) \tag{13}$$

are independent in $H^2_{rig}(U)$, then the forms (13) are a basis for the lattice

$$H(X, \log D) = \mathrm{Im}(H^2_{cris}((X,D)) \to H^2_{rig}(U)).$$

Note that they will be independent in $H^2_{rig}(U)$ if and only if $|S(k)| = \dim H^2_{rig}(U)$; the latter is just $(\dim H^2_{rig}(X) - 1) + \dim H^1_{rig}(D)$ (c.f. first paragraph of the proof of Proposition 6.1), and so is easily calculated.

If $k \geq \max\{2d-4, 0\}$ and the classes of (13) are independent in $H^2_{rig}(U)$, then the classes of (13) span a lattice $H(X, kD) \subset H^2_{rig}(U)$ such that there is a natural embedding $\rho : H(X, \log D) \to H(X, kD)$ with cokernel killed by $p^{\lfloor \log_p(k+1)\rfloor}$. If the classes are not independent in $H^2_{rig}(U)$ then one must do some further work to extract a basis for the free part of $\langle S(k)\rangle_W$. We have not come across this situation in practice and so do not address it here.

5 Frobenius-Hodge structures and precision estimates

In this section we explain how the use of a basis for the full-rank W-lattice $H(X, kD)$ in $H^2_{rig}(U)$ when calculating the Frobenius action allows one to compute with lower p-adic precisions.

Notation and assumptions are as in Section 4. In particular, $\mathcal{X} := \tilde{\mathcal{X}}/G$ where G is a finite group of order prime to p and $\tilde{\mathcal{X}}$ a smooth surface in $\mathbb{P}^3_W$, $\tilde{\mathcal{D}}$ is the divisor at infinity of $\tilde{\mathcal{X}}$,

assumed smooth and fixed by G, and $\mathcal{U} := \tilde{\mathcal{U}}/G$ (where $\tilde{\mathcal{U}} := \tilde{\mathcal{X}}\backslash\tilde{\mathcal{D}}$) is smooth. We denote by X, D and U the special fibres of $\mathcal{X}, \mathcal{D}$ and $\mathcal{U}$, respectively. For $k \geq \max\{2d-4, 0\}$ the W-lattice $H(X, kD) \subset H^2_{rig}(U)$ is described in Definition 4.9.

To state the next theorem in a simple manner, we shall say informally that a rational approximation $\tilde{a} \in \mathbb{Q}$ to a p-adic number $a \in \mathbb{Q}_p$ is correct modulo p^N if $\mathrm{ord}_p(\tilde{a}-a) \geq N$, with this notion extended in the obvious way to matrices and polynomials.

Theorem 5.1. *Assume that the residue field of W is the prime field $\mathbb{F}_p$ where $p > 2$, and denote by $h^{2,0} := \dim H^0(\mathcal{X}_K, \hat{\Omega}^2_{\mathcal{X}_K})$ the geometric genus of $\mathcal{X}_K$ (Definition 4.13). Let $\tilde{A}$ be an approximation to the matrix for the Frobenius map F on $H(X, kD) \otimes_W K$ w.r.t. a basis of $H(X, kD)$ which is correct modulo p^{N+1}, where $N \geq 2$. Then the polynomial $\det(1 - p^{-1}\tilde{A}T)$ is correct modulo $p^{N+1-h^{2,0}-\lfloor \log_p(k+1)\rfloor}$.*

This theorem is surprising since the matrix $p^{-1}\tilde{A}$ will not in general have entries in W, and so one naively expects a much greater loss of precision when the characteristic polynomial is computed. For example, when $p > k+1$ one expects naively that the characteristic polynomial of $p^{-1}\tilde{A}$ is only correct modulo $p^{N+1-(m-1)}$ where m is the dimension of $H^2_{rig}(U)$. In our application to L-functions of elliptic curves, m is much larger than $h^{2,0}$, and so Theorem 5.1 is of great practical use.

Theorem 5.1 is an immediate corollary of the next proposition.

Proposition 5.2. *Let $\mathcal{B}$ be a basis for the W-lattice $H(X, kD)$, and hence also the K-vector space $H(X, kD) \otimes_W K$. Let $A \in \mathrm{GL}(m, K)$ be the matrix for the Frobenius map F acting on $H(X, kD) \otimes_W K$ w.r.t. this basis. Let $N \geq 2$ be a positive integer and $\tilde{A} \in \mathrm{GL}(m, \mathbb{Q})$ be a matrix such that $\mathrm{ord}_p(\tilde{A}-A) \geq N+1$. Write $\det(1-AT) = \sum_{\ell=0}^m a_\ell T^\ell$ and $\det(1-\tilde{A}T) = \sum_{\ell=0}^m \tilde{a}_\ell T^\ell$. Then*

$$\mathrm{ord}_p(a_\ell - \tilde{a}_\ell) \geq N + i + m(\ell) - \lfloor \log_p(k+1)\rfloor$$

where $m(\ell)$ is defined in the proof of Lemma 5.3.

We shall prove this proposition in several simple steps. Using the notation and results in Section 4.2, we have an exact sequence

$$0 \to H(X)_{prim} \xrightarrow{\theta} H(X, \log D) \xrightarrow{\phi} H(D)(-1) \to 0$$

which defines a mixed Frobenius-Hodge structure (Definition 3.12) on $H(X, \log D)$ from the pure Frobenius-Hodge structures on the outer terms. Say that a basis for $H(X)_{prim}$ is adapted to the Hodge filtration if the first $h^{2,0}$ elements form a basis for H_2, and the first $h^{2,0} + h^{1,1} - 1$ form a basis for H_1. Likewise, say that a basis for $H(D)$ is adapted to the Hodge filtration if the first g elements form a basis for H'_1. Say that a basis for $H(X, \log D)$ is adapted to the Hodge filtration if the first $h_2 - 1$ elements are θ applied to a basis of $H(X)_{prim}$ which is adapted to the Hodge filtration, and $p^{-1}\phi$ applied to the last $2g$ elements gives a basis of $H(D)$ which is adapted to the Hodge filtration. Note that $m = (h_2 - 1) + 2g$ is the rank of $H(X, \log D)$.

The matrix A for Frobenius F on a basis of $H(X, \log D)$ which is adapted to the Hodge filtration has the shape

$$\begin{pmatrix} p^2 A_2 & p A_1 & A_0 & B_1 & B_2 \\ 0 & 0 & 0 & p^2 C_1 & p C_2 \end{pmatrix}$$

where $A_0, A_2 \in \mathrm{M}(h_2 - 1, h^{2,0}, W)$, $A_1 \in \mathrm{M}(h_2 - 1, h^{1,1} - 1, W)$, $C_i \in \mathrm{M}(2g, g, W)$, $B_i \in \mathrm{M}(h_2 - 1, g, W)$ and the 0s are zero matrices of the appropriate size.

Lemma 5.3. *Let $\mathcal{B}$ be a basis for $H(X, \log D)$ which is adapted to the Hodge filtration and A the matrix for Frobenius F on $H(X, \log D)$ w.r.t. the basis $\mathcal{B}$. Let $N \geq 2$ be a positive integer and $\tilde{A} \in \mathrm{GL}(m, \mathbb{Q})$ be a matrix such that $\mathrm{ord}_p(\tilde{A}-A) \geq N+1$. Write $\det(1-AT) = \sum_{\ell=0}^m a_\ell T^\ell$ and $\det(1-\tilde{A}T) = \sum_{\ell=0}^m \tilde{a}_\ell T^\ell$. Then*

$$\mathrm{ord}_p(a_\ell - \tilde{a}_\ell) \geq N + i + m(\ell)$$

where $m(\ell)$ is defined in the proof.

Proof. Write $p^{-1}A = (p^{-1}a_{i,j})$ and $p^{-1}\tilde{A} = (p^{-1}\tilde{a}_{i,j})$, so $\mathrm{ord}_p(p^{-1}\tilde{a}_{i,j} - p^{-1}a_{i,j}) \geq N \geq 2$. From the explicit block-form of the matrix A immediately above, one sees that the matrix $V = (v_{i,j})$ below is such that $\mathrm{ord}_p(p^{-1}a_{i,j})$, $\mathrm{ord}_p(p^{-1}\tilde{a}_{i,j}) \geq v_{i,j}$.

$$V := \begin{pmatrix} 1 & \cdots & 1 & 0 & \cdots & 0 & -1 & \cdots & -1 & -1 & \cdots & -1 & -1 & \cdots & -1 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 1 & \cdots & 1 & 0 & \cdots & 0 & -1 & \cdots & -1 & -1 & \cdots & -1 & -1 & \cdots & -1 \\ N & \cdots & N & N & \cdots & N & N & \cdots & N & 1 & \cdots & 1 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ N & \cdots & N & N & \cdots & N & N & \cdots & N & 1 & \cdots & 1 & 0 & \cdots & 0 \end{pmatrix}$$

Explicitly, the top left-hand $(h_2 - 1) \times h^{2,0}$ sub-matrix of 1s in V corresponds to lower bounds on the valuation of entries in the matrix pA_2, and so on. Let $1 \leq \ell \leq m$. The ℓth coefficient of $\det(1 - Tp^{-1}\tilde{A})$ can be written explicitly as a signed sum of transversal products of the elements $p^{-1}\tilde{a}_{i,j}$ in $p^{-1}\tilde{A}$, c.f. [18, Equation (36)]. Each transversal product is determined by a choice of indices $1 \leq u_1 < \cdots < u_\ell \leq m$ and permutation $\tau \in S_\ell$; namely, this defines the term $\mathrm{sign}(\tau)(p^{-1}\tilde{a}_{u_1,u_{\tau(1)}}) \cdots (p^{-1}\tilde{a}_{u_\ell,u_{\tau(\ell)}})$. According to [18, Lemma 9.5], the loss of precision

$$\mathrm{ord}_p((p^{-1}a_{u_1,u_{\tau(1)}}) \cdots (p^{-1}a_{u_\ell,u_{\tau(\ell)}}) - (p^{-1}\tilde{a}_{u_1,u_{\tau(1)}}) \cdots (p^{-1}\tilde{a}_{u_\ell,u_{\tau(\ell)}}))$$

when computing such a product is bounded below by $N + v(u_1, \ldots, u_\ell; \tau)$ where

$$v(u_1, \ldots, u_\ell; \tau) := \sum_{i=1}^{\ell} v_{u_i,u_{\tau(i)}} - \min_{1 \leq i \leq \ell}\{v_{u_i,u_{\tau(i)}}\}.$$

So for each ℓ, we must find the minimum value $m(\ell)$ taken by the function $v(u_1, \ldots, u_\ell; \tau)$ over different choices of indices and permutation. By inspection of the matrix V, one sees that

$$m(\ell) = \begin{cases} -\ell + 1 & 1 \leq \ell \leq h^{2,0} \\ -h^{2,0} + 1 & h^{2,0} < \ell \leq h^{2,0} + h^{1,1} - 1 + g \\ -h^{2,0} + 1 + (\ell - (h^{2,0} + h^{1,1} - 1 + g)) & h^{2,0} + h^{1,1} - 1 + g < \ell \leq m. \end{cases}$$

The key point is that since $N \geq 2$, one can restrict to transversals of $p^{-1}A$ which factor as a transversal of the $(h_2 - 1) \times (h_2 - 1)$ sub-matrix $(pA_2, A_1, p^{-1}A_0)$ times one of the $2g \times 2g$ sub-matrix (pC_1, C_2), and it is easy to compute the minimum value of $v(\cdot)$ over such transversals. To see why we can restrict in this way, suppose that $1 \leq u_1 < \cdots < u_\ell \leq m$ is a choice of indices and $\tau \in S_\ell$ permutation such that the corresponding transversal of $p^{-1}A$ contains exactly $s \geq 1$ elements from the top-right $h_2 - 1 \times 2g$ sub-matrix of $p^{-1}A$. Then by Lemma 5.4, the transversal must also contain exactly s elements from the bottom-left $2g \times h_2 - 1$ sub-matrix of $p^{-1}A$. Hence $v(u_1, \ldots, u_\ell; \tau)$ equals $(N-1)s \geq s$ plus a choice of $\ell - s$ elements lying in distinct columns (and rows) of the top-left $h_2 - 1 \times h_2 - 1$ sub-matrix of V and the bottom-right $2g \times 2g$ submatrix of V, plus one. Such a sum cannot be less than the value $m(\ell)$ given above. $\square$

Lemma 5.4. *Let M be an $m \times m$ matrix over a commutative ring and $M = (M_{ij})_{1 \leq i,j \leq 2}$ a block decomposition where the block $M_{1,1}$ is square of size m', and the block $M_{2,2}$ is square of size $m'' := m - m'$. Then any transversal product of M must contain an equal number of elements from $M_{1,2}$ and $M_{2,1}$. (See the proof of Lemma 5.3 for a definition of the term transversal product.)*

Proof. We may restrict immediately to the case in which the transversal product is determined by choosing an element from every row and column of M, by extracting a suitable submatrix. For such a transversal product, if s elements are chosen from $M_{1,2}$ then by considering columns one sees $m'' - s$ are chosen from $M_{2,2}$, and by considering rows that $m' - s$ are chosen from $M_{1,1}$. Hence $m - (s + (m' - s) + (m'' - s)) = s$ are chosen from $M_{2,1}$. $\square$

Lemma 5.5. *Lemma 5.3 is true for $\mathcal{B}$ any basis of $H(X, \log D)$.*

Proof. Let $\mathcal{B}$ be any basis for $H(X, \log D)$ and A the matrix for Frobenius F w.r.t. $\mathcal{B}$. Let $\mathcal{B}'$ be a basis adapted to the Hodge filtration and A' the matrix for Frobenius F w.r.t. $\mathcal{B}'$. Of course, the characteristic polynomials of A and A' are the same. Let $\tilde{A} \in \mathrm{GL}(\mathbb{Q}, m)$ be such that $\mathrm{ord}_p(\tilde{A} - A) \geq N + 1$. Let $C \in \mathrm{GL}(m, W)$ be the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$, so $A' = C^{-1}AC$. Define $D := C^{-1}\tilde{A}C$, so the characteristic polynomials of D and $\tilde{A}$ are identical. We have $D - A' = C^{-1}(\tilde{A} - A)C$ so $\mathrm{ord}_p(D - A') \geq N + 1$. Hence the characteristic polynomials of D and A' agree as claimed in Lemma 5.3. Thus so do those of $\tilde{A}$ and A. $\square$

Lemma 5.6. *Proposition 5.2 is true for bases $\mathcal{B}$ of $H(X, kD)$ which satisfy the following property: There exists a basis $\mathcal{B}'$ of $H(X, \log D)$ with the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$ a diagonal matrix $E = \mathrm{diag}(p^{n_1}, \ldots, p^{n_m})$ with $n_i \leq \lfloor \log_p(k+1) \rfloor$.*

Note that such bases exist since we know that $H(X, kD)/H(X, \log D)$ is a finite abelian p-group killed by multiplication by $p^{\lfloor \log_p(k+1) \rfloor}$.

Proof. Define $G := E^{-1}\tilde{A}E$ and $H := E^{-1}AE$. Then H is the matrix for Frobenius F w.r.t. a basis of the lattice $H(X, \log D)$. Moreover, $G - H = E^{-1}(\tilde{A} - A)E$ and so $\mathrm{ord}_p(G - H) \geq (N + 1) - \lfloor \log_p(k+1) \rfloor$. The characteristic polynomials of G and H are the same as those of $\tilde{A}$ and A, respectively, that is $\sum_{i=0}^m \tilde{a}_i T^i$ and $\sum_{i=0}^m a_i T^i$. By Lemma 5.5 (with notation "A and $\tilde{A}$" replaced by "H and G", and N replaced by $N - \lfloor \log_p(k+1) \rfloor$) they agree as claimed. $\square$

One now deduces Proposition 5.2 from Lemma 5.6 using a similar argument as that in the proof of Lemma 5.5.

6   The inclusions $U \subset X$ and $V \subset U$

In this section we analyse the kernel and cokernel of the map $H^n_{rig}(U) \to H^n_{rig}(V)$ which arises in the fibration method. We restrict to the case in which $n = 2$ and $H^1_{rig}(X) = 0$. The actual practical computation of this map does not cause any problems. Since both U and V are affine, cohomology classes can be represented by n-forms defined globally, and the map is just restriction.

We also briefly consider the problem of computing the residue map Res in the exact sequence

$$\cdots \to H^n_{cris}(X) \to H^n_{cris}((X, D)) \overset{Res}{\to} H^{n-1}_{cris}(D)(-1) \to \cdots .$$

Given a basis for the full rank W-lattice $H(X, \log D) = \mathrm{Im}(H^n_{cris}(X, D) \to H^n_{rig}(U))$, the sublattice $H(X)_{prim} \subseteq H(X, \log D)$ can in principle be recovered through an understanding of the residue map (Step 2 in Section 2.3.3).

6.1   Excision exact sequences

In this section we gather some exact sequences which will be used in Section 6.2 and have already been used in some earlier sections. First, for Y a smooth projective variety over $\mathbb{F}_q$ and Z a smooth normal crossings divisor, we have the "residue" sequence

$$\cdots \to H^i_{cris}(Y) \to H^i_{cris}((Y, Z)) \overset{Res}{\to} H^{i-1}_{cris}(Z)(-1) \to \cdots . \tag{14}$$

(This follows, in the case in which the pair (Y, Z) lifts to a smooth pair over W at least, from the analogous sequence in algebraic de Rham cohomology [1, Proposition 2.2.8] and the comparision theorems [1, Definition 2.3.3, Proposition 2.4.1].) Second, for Y a smooth variety over $\mathbb{F}_q$ of pure dimension d and $Z \subset Y$ a closed subscheme we have the localisation sequence

$$\cdots \to H^i_{Z,rig}(Y) \to H^i_{rig}(Y) \to H^i_{rig}(Y \backslash Z) \to \cdots .$$

Here $H^i_{Z,rig}(Y)$ is rigid cohomology of Y with support along Z, which is really just defined to make this sequence exact. When Z is smooth and pure of codimension e, one has the Gysin isomorphism [25]

$$H^i_{rig,Z}(Y) \cong H^{i-2e}_{rig}(Z)(-e)$$

which leads to the more useful sequence

$$\cdots \to H^{i-2e}_{rig}(Z)(-e) \to H^i_{rig}(Y) \to H^i_{rig}(Y \backslash Z) \to \cdots . \tag{15}$$

Sequences (14) and (15) are related in so much as if one tensors the first by K over W one obtains a special case of the second. We only need (15) for our application in the next section. Finally, we recall that when Y is affine $H^i_{rig}(Y) = 0$ for $i > \dim(Y)$.

6.2   Injectivity of the map $H^2_{rig}(U) \to H^2_{rig}(V)$

The propositions in this section makes rigorous the ideas in [18, Section 9.3.1]. First, we consider the case of a smooth surface X.

Proposition 6.1. *Let X be a smooth projective surface over $\mathbb{F}_q$, with $H^1_{rig}(X) = H^3_{rig}(X) = 0$, U an affine piece of X obtained by removing a smooth divisor D, and $V \subset U$ such that $Z := U \backslash V$ is pure of dimension 1 and there is a map $V \to S \subset \mathbb{A}^1$ with smooth fibres. Then the map $H^2_{rig}(U) \to H^2_{rig}(V)$ is an injection.*

Proof. Writing out the sequence (15) in full for the pair (X, D) one obtains

$$
\begin{array}{ccccccc}
0 & \to & H^0_{rig}(X) & \to & H^0_{rig}(U) & \to & 0 \\
 & \to & 0 & \to & H^1_{rig}(U) & \to & H^0_{rig}(D)(-1) \\
 & \overset{c}{\to} & H^2_{rig}(X) & \to & H^2_{rig}(U) & \to & H^1_{rig}(D)(-1) \\
 & \to & 0 & \to & 0 & \to & H^2_{rig}(D)(-1) \\
 & \to & H^4_{rig}(X) & \to & 0 & \to & 0.
\end{array}
$$

Note that $H^0_{rig}(X) = H^0_{rig}(D) = K$. The image of the map c is the class of the divisor D. Since the cycle class map is injective in codimension one [23, Page 97], we must have that $H^1_{rig}(U) = 0$.

Let $V \subset U$ with $Z := U \backslash V$ pure of codimension 1. We do not assume that Z is smooth, so cannot apply the sequence (15) directly to the pair (U, Z). To get around this problem: Let P denote the singular locus on Z, a union of points, and $\tilde{Z} := Z \backslash P$, $\tilde{U} := U \backslash P$. First, (U, P) is a smooth pair, with P of codimension 2 in U. So (15) for this pair is

$$
\begin{array}{ccccccc}
0 & \to & 0 & \to & H^0_{rig}(U) & \to & H^0_{rig}(\tilde{U}) \\
 & \to & 0 & \to & H^1_{rig}(U) & \to & H^1_{rig}(\tilde{U}) \\
 & \to & 0 & \to & H^2_{rig}(U) & \to & H^2_{rig}(\tilde{U}) \\
 & \to & 0 & \to & 0 & \to & H^3_{rig}(\tilde{U}) \\
 & \to & H^0_{rig}(P)(-2) & \to & 0 & \to & 0
\end{array}
$$

Note that $\tilde{U}$ is not affine when $P \neq \emptyset$. Second, $(\tilde{U}, \tilde{Z})$ is a smooth pair with $\tilde{Z}$ of codimension 1 in $\tilde{U}$ and $V = \tilde{U} \backslash \tilde{Z}$. So (15) for this pair is

$$
\begin{array}{ccccccc}
0 & \to & 0 & \to & H^0_{rig}(\tilde{U}) & \to & H^0_{rig}(V) \\
 & \to & 0 & \to & H^1_{rig}(\tilde{U}) & \to & H^1_{rig}(V) \\
 & \to & H^0_{rig}(\tilde{Z})(-1) & \to & H^2_{rig}(\tilde{U}) & \to & H^2_{rig}(V) \\
 & \to & H^1_{rig}(\tilde{Z})(-1) & \to & H^3_{rig}(\tilde{U}) & \to & 0
\end{array}
$$

Thus the following sequence is exact

$$0 \to H^1_{rig}(V) \to H^0_{rig}(\tilde{Z})(-1) \to H^2_{rig}(U) \to H^2_{rig}(V)$$

$$\to H^1_{rig}(\tilde{Z})(-1) \to H^0_{rig}(P)(-2) \to 0. \tag{16}$$

21

To calculate $H_{rig}^i(V)$ for $i = 1, 2$, we use the assumption that there is a surjective map $V \to S \subset \mathbb{A}^1$ with smooth fibres. Let $H_{rig}^i(V/S)$ denote relative rigid cohomology for this map, where $i = 0, 1, 2$. Then

$$H_{rig}^1(V) \cong E_{2,rig}^{0,1} \oplus E_{2,rig}^{1,0}, \quad H_{rig}^2(V) \cong E_{2,rig}^{1,1}$$

where

$$
\begin{aligned}
E_{2,rig}^{1,i} &:= \operatorname{Coker}\left(\nabla : H_{rig}^i(V/S) \to H_{rig}^i(V/S) \otimes \Omega_S^1\right). \\
E_{2,rig}^{0,1} &:= \operatorname{Ker}\left(\nabla : H_{rig}^1(V/S) \to H_{rig}^1(V/S) \otimes \Omega_S^1\right).
\end{aligned}
$$

As in the proof of [18, Proposition 8.1] we have $E_{2,rig}^{1,0} \cong H_{rig}^1(S)(-1)$ and one sees $H_{rig}^1(S) \cong H_{rig}^0(\tilde{Z})$. Thus (16) begins

$$0 \to E_{2,rig}^{0,1} \oplus H_{rig}^1(S)(-1) \to H_{rig}^1(S)(-1) \to H_{rig}^2(U) \to \cdots$$

and we deduce that $E_{2,rig}^{0,1} = 0$ and $H_{rig}^2(U) \hookrightarrow H_{rig}^2(V)$.

Our conclusion is that the following sequence is exact

$$0 \to H_{rig}^2(U) \to H_{rig}^2(V) \to H_{rig}^1(\tilde{Z})(-1) \to H_{rig}^0(P)(-2) \to 0$$

and in particular the map $H_{rig}^2(U) \hookrightarrow H_{rig}^2(V)$ is an injection. $\qquad\square$

Next, we consider the case which arises in our application; that of a quasi-smooth hypersurface in a weighted projective space.

Proposition 6.2. *As in Section 4, let $X := \tilde{X}/G$ where G is a finite group of order prime to p and $\tilde{X}$ a smooth surface in $\mathbb{P}_{\mathbb{F}_q}^3$. Let $\tilde{D}$ be the divisor at infinity of $\tilde{X}$, assumed smooth and fixed by G, and $U := \tilde{U}/G$ where $\tilde{U} := \tilde{X} \setminus \tilde{D}$. Furthermore, let $V \subset U$ be such that $Z := U \setminus V$ is pure of dimension 1, and there is a map $V \to S \subset \mathbb{A}^1$ with smooth fibres. Then the map $H_{rig}^2(U) \to H_{rig}^2(V)$ is an injection.*

Proof. The proof is as before, once one has established that $H_{rig}^1(U) = 0$. Now $H_{rig}^1(\tilde{X}) = 0$ since $\tilde{X}$ is a smooth hypersurface in $\mathbb{P}_{\mathbb{F}_q}^3$. The sequence (15) for the pair $(\tilde{X}, \tilde{D})$ reveals that $H_{rig}^1(\tilde{U}) = 0$. Hence $H_{rig}^1(U) = H_{rig}^1(\tilde{U})^G = 0$, as required. $\qquad\square$

6.3 Computing the residue map

In principle the residue map can be computed by using explicit Čech-de Rham complexes, following the approach of Gerkmann [10]. In unpublished notes, the author refined Gerkmann's work to obtain an explicit formula for the residue map in the case in which $\mathcal{X} := \mathbb{P}_W^2$ and $\mathcal{D}$ is a curve. Extending this to the case $\mathcal{X} := \mathbb{P}_W^3$ and $\mathcal{D}$ is a surface proved too challenging for the present author, although plausible explicit expressions were obtained after much work. Note that the author carried out these latter calculations in an attempt to recover the lattice $\operatorname{Im}(H_{cris}^2(D) \to H_{rig}^2(D))$ from the construction in [1] of the lattice $\operatorname{Im}(H_{cris}^3((X, D)) \to H_{rig}^3(X \setminus D))$ via the residue map.

The author's experience with these calculations suggest that the explicit construction of the residue map in the case $\mathcal{X}$ is a surface and $\mathcal{D}$ is a smooth divisor is in principle possible, but perhaps not desirable in practice unless $H_{rig}^2(U)$ has much larger dimension than $\operatorname{Im}(H_{rig}^2(X) \to H_{rig}^2(U))$. In our calculations in Section 9 the former had dimension only two greater than the latter.

7 The Fuchsian basis problem

This section is entirely expositional. We introduce the Fuchsian basis problem, and explain its relevance to our algorithm.

7.1 Hilbert's 21st problem and Fuchsian bases

Let F be a field of characteristic zero and consider a linear differential system

$$\frac{dC(y)}{dy} + B(y)C(y) = 0, \tag{17}$$

where $B(y)$ is an $m \times m$ matrix with entries in the rational function field $F(y)$, and the solution matrix $C(y)$ is an invertible matrix over some differential extension field of $F(y)$. If $H(y)$ is any invertible matrix of rational functions, we may transform (17) into an equivalent differential system in which B is replaced by

$$B_{[H]} := H^{-1}BH + H^{-1}\frac{dH}{dy}. \tag{18}$$

For an irreducible polynomial $p(y) \in F[y]$ let $F(y)_p := F(y)[1/p]$ and $F(y)_{(p)}$ denote the local ring at p, i.e., the extension of $F[y]$ in which all irreducible polynomials *excluding* $p(y)$ have been inverted. We shall say that (17) is *regular* at $p(y) \in F[y]$ if there exists a matrix $H \in GL(m, F(y)_p)$ such that $B_{[H]}$ has entries in $F(y)_{(p)}$. We shall say that (17) is *regular singular* at $p(y) \in F[y]$ if it is not regular at $p(y)$ but there exists a matrix $H \in GL(m, F(y)_p)$ such that $p(y)B_{[H]}$ has entries in $F(y)_{(p)}$. We say that the system is regular/regular singular at infinity, if is regular/regular singular at y, after replacing the matrix $B(y)$ by $-1/y^2 B(1/y)$. We call (17) *regular singular* if it is either regular or regular singular at all irreducible polynomials $p(y)$ and infinity.

For simplicity of exposition, let us henceforth assume that the system (17) is regular singular at infinity, and let $P(y)$ be the product of all irreducible polynomials $p(y)$ at which it is regular singular. Let us say $P(y)$ defines the finite singular locus. We shall say that (17) is *Fuchsian* if there exists a matrix $H \in GL(m, F[y, 1/P(y)])$ such that $P(y)B_{[H]}$ has entries in $F[y]$ of degree less than $\deg(P(y))$. We call $B_{[H]}$ of this form a *Fuchsian matrix* for the differential system (17). Fuchsian systems are of course regular singular. Establishing whether the converse holds when F is the field of complex numbers is closely related to Hilbert's 21st problem, though not the statement of it. We require a solution to the problem:

Fuchsian Basis Problem. *Give an algorithm which takes as input a regular singular differential system (17) which is regular singular at infinity and has finite singular locus defined by the polynomial $P(y)$, and either*

- *Gives as output a change of basis matrix $H(y) \in GL(m, F[y, 1/P(y)])$ such that $B_{[H]}$ defined in (18) is a Fuchsian matrix for (17),*

- *Terminates and declares correctly that the system is not Fuchsian.*

Hilbert's 21st problem has a chequered but fascinating history. When F is the field of complex numbers, Fuchsian bases are known to exist for regular singular differential systems under various conditions, such as irreducibility. For $m = 3$ there are examples of reducible systems which are regular singular but not Fuchsian; Bolibruch has made a very explicit study of this case [3]. For $m = 2$, all regular singular systems over algebraically closed fields are Fuchsian, and an effective algorithm exists for finding Fuchsian bases (Dekkers's algorithm [5]).

7.2 Picard-Fuchs systems

Let $\mathcal{V}_K \to \mathcal{S}_K \subset \mathbb{P}^1_K$ be a smooth family of K-varieties of relative dimension $n-1$. Associated to this family is a free module $H^{n-1}_{dR}(\mathcal{V}_K/\mathcal{S}_K)$ of finite rank m, say, over the coordinate ring $A := \Gamma(\mathcal{S}_K, \mathcal{O}_{\mathcal{S}_K})$, and an additive and Leibniz linear map (Gauss-Manin connection)

$$\nabla : H^{n-1}_{dR}(\mathcal{V}_K/\mathcal{S}_K) \to H^{n-1}_{dR}(\mathcal{V}_K/\mathcal{S}_K) \otimes_A \Omega^1_A.$$

Choose a coordinate function y on $\mathcal{S}_K$, and basis $e_1, \ldots, e_m$ for $H^{n-1}_{dR}(\mathcal{V}_K/\mathcal{S}_K)$. Then with respect to the choice of bases $\{e_i\}$ and $\{e_i \otimes dy\}$ for the domain and codomain of ∇, the map acts as

$$\frac{d}{dy} + B(y) : A^m \to A^m$$

for some matrix $B(y)$ with entries in A. The differential system associated to the Gauss-Manin connection and choice of initial basis $\{e_i\}$ and coordinate y is defined to be (17). This system is regular singular, and has rational local exponents, by the regularity and local monodromy theorems [12]. The method developed in [18, Section 4] for computing in the cokernel of ∇, and controlling the loss of p-adic precision which accrues, assumes that a basis has been chosen such that the matrix $B(y)$ for the Gauss-Manin connection is Fuchsian.

8 Hyperelliptic curves over the rational function field

In this section we tie up various ends which were left loose in [18]. Specifically, in that paper the author made a conjecture, the truth of which would improve the practical performance of the fibration method for hyperelliptic curves. This conjecture is proved in Section 8.2. Second, the algorithm assumed that certain local monodromy assumptions held true [18, Section 7.4]. In practice, it is easy to check computationally whether these assumptions hold, and they always do. We prove that these assumptions are true for the elliptic curves we consider in Section 9 by an explicit calculation (Section 8.3). Finally, in Section 8.4 we state some results on the complexity of the fibration method, incorporating the various refinements in this paper.

8.1 Notation

Let us first introduce the notation which we shall use in this section. Let q be a power of an odd prime p, and $\bar{Q}(x, y) \in \mathbb{F}_q[x, y]$ have degree $2g + 1$ in the variable x for some integer $g \geq 1$. Denote by $\bar{\Delta}(y)$ the Sylvester resultant of the polynomials $\bar{Q}$ and $\partial \bar{Q}/\partial x$ with respect to the variable x. We assume $\bar{\Delta}(y)$ is non-constant. Let $Q(x, y) \in W[x, y]$ be some lift of the polynomial $\bar{Q}(x, y)$, and Δ the Sylvester resultant of Q and $\partial Q/\partial x$ w.r.t. x. We need to choose $Q(x, y)$ so that $\deg(\Delta) = \deg(\bar{\Delta}) > 0$. This can certainly be done under some hypotheses, which are stated in the results below. Let

$$U := \mathrm{Spec}\left(\mathbb{F}_q[x, y, z]/(z^2 - \bar{Q}(x, y))\right),$$

and let $V \to S$ be the family obtained by taking "Spec" of the homomorphism

$$\mathbb{F}_q[y, 1/\bar{\Delta}(y)] \hookrightarrow \mathbb{F}_q[x, y, 1/\bar{\Delta}(y), z]/(z^2 - \bar{Q}(x, y)).$$

We assume that U is smooth.

In our discussion of complexity estimates in Section 8.4, we assume that U compactifies to a quasi-smooth surface X in a weighted projective space subject to certain further conditions, exactly as in Section 4.3, so that we may use W-lattices in $H^2_{rig}(U)$ to speed-up computations. However, this compactification plays no role in Sections 8.2 and 8.3.

8.2 A conjecture on the relative Frobenius matrix

In this section we prove [18, Conjecture 7.4]. This gives a useful practical improvement to the performance of the fibration method for hyperelliptic curves over function fields $\mathbb{F}_q(y)$.

8.2.1 Statement of conjecture 7.4

We recall some notions from [18, Section 7], alerting the reader again to the fact that our notation has changed. Define $A^\dagger$ to be the weak completion of the coordinate ring of the lifting $\mathcal{S}_K$ of the base S. That is

$$A^\dagger := \left\{ \sum_{i=-\infty}^{\infty} \frac{a_i(y)}{\Delta(y)^i} \mid \deg(a_i) < \deg(\Delta), \, \mathrm{ord}_p(a_i) - \varepsilon|i| \to \infty \text{ for some } \varepsilon > 0 \right\}.$$

There is a lifting of the pth power map from $\mathbb{F}_q[y, 1/\bar{\Delta}(y)]$ to $A^\dagger$ which sends $x \mapsto x^p$ and $y \mapsto y^p$, unique up to a choice of sign. Let us denote this map by $\sigma_{A^\dagger}$. There is a rank $2g$ free module

24

$H^1_{rig}(V/S)$ over $A^\dagger$ with basis given by the classes of the forms $x^i dx/z$ for $i = 0, 1, \ldots, 2g-1$. There is a map $F : H^1_{rig}(V/S) \to H^1_{rig}(V/S)$ which is $\sigma_{A^\dagger}$-linear, called the pth power (relative) Frobenius map. We represent this map F by a matrix $F(y)$ w.r.t. our choice of basis.

[**18, Conjecture 7.4**] *The matrix $F(y)$ has a pole of finite order at $y = \infty$.*

8.2.2   Elliptic curves

Assume that $\bar{Q}(x, y) := x^3 + \bar{a}(y)x + \bar{b}(y)$ for some $\bar{a}(y), \bar{b}(y) \in \mathbb{F}_q[y]$. Then $\bar{\Delta} = 4\bar{a}^3 + 27\bar{b}^2$. We first consider a special case.

Theorem 8.1. *Assume that $\deg(\bar{a}) \le 4e$ and $\deg(\bar{b}) \le 6e$ for some $e \ge 1$, and $\deg(\bar{\Delta}) = 12e$. Then the entries in matrix $F(y)$ when expanded locally as Laurent series in $K((1/y))$ have degree in y at most $(p+1)e$; that is, the pole order of $F(y)$ at $y = \infty$ is bounded by $(p+1)e$.*

Proof. First, lift the elliptic curve equation to get $z^2 = x^3 + a(y)x + b(y)$ where $a, b \in W[y] \subset K(y)$ with $\deg(a) \le 4e$, $\deg(b) \le 6e$ and $\Delta := 4a^3 + 27b^2$ such that $\deg(\Delta) = 12e$. Note that any lifting satisfying the degree restrictions on a and b will be suitable. We make the change of variables $v := 1/y, u := v^{2e}x$ and $w := v^{3e}z$ to get an equation $w^2 = u^3 + \tilde{a}(v)u + \tilde{b}(v)$. Here $\tilde{a}(v) := v^{4e}a(1/v) \in W[v]$ and $\tilde{b}(v) := v^{6e}b(1/v) \in W[v]$. The condition on the degree of the discriminant ensures us that $\tilde{\Delta}(v) := 4\tilde{a}^3 + 27\tilde{b}^2 = v^{12e}\Delta(1/v)$ does not vanish at $v = 0$, even modulo p. So the lifted curve over $W[v]$ has good reduction at $v = 0$, even modulo p. Recall that d is the universal derivation of the function field of the generic fibre of the lifted curve over the base field $K(y) = K(v)$. We see that

$$\frac{dx}{z} = v^e \frac{du}{w}, \ \frac{xdx}{z} = v^{-e}\frac{udu}{w} \ \text{and} \ \frac{du}{w} = y^e\frac{dx}{z}, \ \frac{udu}{w} = y^{-e}\frac{xdx}{z}. \tag{19}$$

The matrix $F(y)$ expresses the action of the pth power Frobenius map on the basis dx/z and xdx/z. Let $F_{ij}(y)$ be the (i, j)th entries in $F(y)$, for $1 \le i, j \le 2$. These are p-adic functions which converge on some open annulus of outer radius 1 around $y = \infty$. We wish to show that they only have a finite polynomial part in y; that is, they converge on the punctured open unit disk around $y = \infty$. Letting σ denote the Frobenius action on functions and differentials we have

$$\sigma\left(\frac{dx}{z}\right) = \sigma\left(v^e\frac{du}{w}\right) = v^{ep}\sigma\left(\frac{du}{w}\right).$$

The expression $\sigma\left(\frac{du}{w}\right)$ may be computed using Kedlaya's method [18, Section 7.3.3], and written modulo exact differentials as a linear combination

$$\sigma\left(\frac{du}{w}\right) \equiv A_{1,1}(v)\frac{du}{w} + A_{1,2}(v)\frac{udu}{w}.$$

The key point is that $A_{1,1}(v), A_{1,2}(v) \in K[[v]]$; thus these functions do not have poles at $v = 0$. The reason for this is that since the lifted curve modulo p is smooth at $v = 0$, Kedlaya's reduction formulae do not introduce poles at this point. (Kedlaya's explicit method only introduces poles at singular fibres; indeed one can adapt this proof to show poles do not occur at singular fibres with potentially good reduction.) Similarly, we see that

$$\sigma\left(\frac{xdx}{z}\right) = v^{-ep}\sigma\left(\frac{udu}{w}\right) \equiv v^{-ep}\left(A_{2,1}(v)\frac{du}{w} + A_{2,2}(v)\frac{udu}{w}\right)$$

where $A_{2,1}(v), A_{2,2}(v) \in K[[v]]$. Hence using (19) to get back to our original basis we find

$$\begin{aligned}
F_{1,1} &= y^{-ep}A_{1,1}(1/y)y^e, \quad F_{1,2} = y^{-ep}A_{1,2}(1/y)y^{-e}, \\
F_{2,1} &= y^{ep}A_{1,2}(1/y)y^e, \quad\ \ F_{2,2} = y^{ep}A_{2,2}(1/y)y^{-e}
\end{aligned}$$

where $A_{i,j} \in K[[1/y]]$. Thus the matrix $F(y)$ has no positive powers of y in the $(1, 1)$ and $(1, 2)$ positions, degree in y bounded by $(p+1)e$ in the $(2, 1)$ position, and degree bounded by $(p-1)e$ in the $(2, 2)$ position. $\square$

The bounds in the theorem above on the pole order for the elliptic curves considered in Section 9 are $(p+1)e$ where $p = 7$ and $e \in \{1, 2, 3, 4, 5\}$, that is $8, 16, 24, 32, 40$, and the actual pole orders observed were $6, 12, 18, 24, 30$, respectively.

We now consider the general case.

Theorem 8.2. *Assume $\deg(\bar{a}) \leq d/3$ and $\deg(\bar{b}) \leq d/2$ where the discriminant $\bar{\Delta} := 4\bar{a}^3 + 27\bar{b}^2$ has degree $d \geq 1$. Then the entries in matrix $F(y)$ when expanded locally as Laurent series in $K((1/y))$ have degree in y at most $\lfloor (p+1)d/12 \rfloor$; that is, the pole order of $F(y)$ at $y = \infty$ is bounded by $\lfloor (p+1)d/12 \rfloor$.*

Proof. Lift the curve as before, preserving the degree of the discriminant. Let m be the smallest integer such that $12|md$ where $d = \deg(\Delta(y))$. Define $\tilde{y} := y^{1/m}$ and consider the generic fibre of the original lifted curve as being defined by the equation $z^2 = x^3 + a(\tilde{y}^m)x + b(\tilde{y}^m)$ over the totally ramified extension $K(\tilde{y})/K(y)$. Then $\deg_{\tilde{y}}(\Delta(\tilde{y}^m)) = 12e$ for some integer $e \geq 1$. Now proceed as in the proof of Theorem 8.1, via the change of variables $v := 1/\tilde{y}, u := v^{2e}x$ and $w := v^{3e}z$, to deduce that the Frobenius matrix $F(\tilde{y})$ has degree in $\tilde{y}$ bounded by $(p+1)e$. But this matrix converges on an open annulus around infinity, and so must have entries in $K((1/y))$. Thus we deduce that the pole order at $y = \infty$ of $F(y)$ is bounded by $\lfloor (p+1)e/m \rfloor = \lfloor (p+1)d/12 \rfloor$. $\square$

Applying the above theorem to [18, Examples 9.1, 9.2], one obtains bounds on the pole order of $\lfloor (17+1)26/12 \rfloor = 39$ and $\lfloor (5+1)62/12 \rfloor = 31$, respectively, which are exactly the pole orders observed experimentally.

8.2.3 Hyperelliptic curves

The same technique can be used to prove [18, Conjecture 7.4] in greater generality; that is, first consider the case when the fibre $y = \infty$ is smooth, using an explicit change of basis, and then make a totally ramified extension of $K(y)$ to reduce to this case. We need the following lemma.

Lemma 8.3. *Let $g \geq 0$ and $\mathbb{Z}[a_2, a_4, \ldots, a_{2(2g+1)}]$ be a graded polynomial ring, where $\mathrm{wt}(a_i) := i$. Then the discriminant of the polynomial $x^{2g+1} + a_2 x^{2g} + a_4 x^{2g-1} + \cdots + a_{4g}x + a_{2(2g+1)}$ is homogeneous of degree $2(2g+1)2g$.*

Proof. For $\lambda \in \mathbb{Q}^*$ the zero locus of the discriminant is invariant under the map $a_{2i} \mapsto \lambda^i a_{2i}$ ($1 \leq i \leq 2g+1$), since on the original polynomial this transformation composed with $x \to \lambda x$ is just multiplication by λ^{2g+1}. So the discriminant is weighted homogeneous w.r.t. the given weights. To compute the degree, specialise all but the constant coefficient to zero and use the explicit expression as the discriminant as the determinant of a Sylvester matrix. $\square$

The next theorem subsumes Theorem 8.2.

Theorem 8.4. *Let $\bar{Q}(x, y) \in \mathbb{F}_q[x, y]$ be monic of degree $2g + 1$ in the variable x for some integer $g \geq 1$. Let $\bar{\Delta}(y)$ be the discriminant of the hyperelliptic curve $z^2 = \bar{Q}(x, y)$ over $\mathbb{F}_q(y)$, and $d := \deg(\bar{\Delta}) > 0$. Assume that when one writes $\bar{Q}(x, y) = x^{2g+1} + \bar{a}_2(y)x^{2g} + \bar{a}_4(y)x^{2g-1} + \cdots + \bar{a}_{2(2g+1)}(y)$ we have*

$$\deg_y(\bar{a}_i(y)) \leq d\frac{i}{2(2g+1)2g}.$$

Then the entries in the matrix $F(y)$ when expanded locally as Laurent series in $K((1/y))$ have degree in y at most $\lfloor d(2g-1)(p+1)/(4(2g+1)g) \rfloor$; that is, the pole order of $F(y)$ at $y = \infty$ is bounded by $\lfloor d(2g-1)(p+1)/(4(2g+1)g) \rfloor$.

Proof. Lift the polynomial $\bar{Q}(x, y)$ to a polynomial $Q(x, y) \in W[x, y]$ preserving the discriminant degree. Lemma 8.3 and the assumptions on the degrees of the coefficients $\bar{a}_i(y)$ assures us that any lifting which preserves the degree bounds on the coefficients will be suitable. Let us first assume that $d = 2(2g+1)2ge$ for some integer e. Define $v := 1/y$, $u := v^{2e}x$ and $w := v^{(2g+1)e}z$. Let $\tilde{Q}(u, v) \in K[u, v]$ be defined as $\tilde{Q}(u, v) := v^{d/2g}Q(v^{-2e}u, 1/v)$. Then the equation $w^2 = \tilde{Q}(u, v)$ defines the generic fibre of the original lifted curve over $K(v)$ w.r.t. the

new choice of variables. The discriminant $\tilde{\Delta}(v)$ of the polynomial $\tilde{Q}(u,v)$ equals $v^d\Delta(1/v)$. Since we preserved the degree of the discriminant when lifting, $\tilde{\Delta}(0) \neq 0$, even modulo p, and the fibre at $v = 0$ is smooth, even modulo p. We can compute the action of F on the new basis $u^i du/w$ for $0 \leq i < 2g$ using Kedlaya's algorithm. Let the (i,j)th coefficients of the matrix thus obtained be $A_{i,j}(v)$. Since the fibre at $v = 0$ is smooth, we have that the local expansions of the functions $A_{i,j}(v)$ at $v = 0$ lie in $K[[v]]$.

Let $F_{i,j}(y)$ be the (i,j)th coefficient of the matrix for the action of F on the original basis $x^i dx/z$, $0 \leq i < 2g$. Using the formulae

$$\frac{x^i dx}{z} = v^{(2g+1)e-2e(i+1)}\frac{u^i du}{w}, \quad \frac{u^j du}{w} = y^{(2g+1)e-2e(j+1)}\frac{x^j dx}{z}$$

we see that

$$F_{i,j}(y) = y^{-p[(2g+1)e-2e(i+1)]}y^{(2g+1)e-2e(j+1)}A_{i,j}(1/y)$$
$$= y^{2e(p(i+1)-(j+1))-(p-1)e(2g+1)}A_{i,j}(1/y).$$

Thus the maximum degree in y which occurs is bounded by

$$2e(2gp-1) - (p-1)e(2g+1) = e(2g-1)(p+1).$$

The general case is treated by first making the change of variable $\tilde{y} := y^{1/m}$ where m is the smallest integer such that $2(2g+1)2ge = md$ for some integer e. One deduces that the degree in $\tilde{y}$ of the matrix $F(\tilde{y})$ is bounded by $e(2g-1)(p+1)$. Hence the degree of $F(y)$ in y is bounded by $\lfloor e(2g-1)(p+1)/m \rfloor = \lfloor d(2g-1)(p+1)/(4(2g+1)g) \rfloor$. $\qquad\square$

Applying the above theorem to [18, Example 9.3] one obtains a bound of $\lfloor 28(4-1)(11+1)/(4(4+1)2) \rfloor = 25$ and the experimentally observed pole order is 21.

8.3 The Gauss-Manin connection for elliptic curves

Write $\bar{Q}(x,y) = x^3 + \bar{a}(y)x + \bar{b}(y)$ and $Q(x,y) = x^3 + a(y)x + b(y)$, with other notation as in Section 8.1. Denote by $B(y)$ the matrix for the Gauss-Manin connection on $H^1_{dR}(\mathcal{V}_K/\mathcal{S}_K)$ with respect to the coordinate function y and initial basis the cohomology classes of dx/z and xdx/z, see Section 7.2 or [18, Section 7.3.1].

Proposition 8.5. *The matrix for the Gauss-Manin connection with respect to our choice of basis, acting on the left on column vectors, is*

$$B(y) = \frac{1}{\Delta(y)}\begin{pmatrix} -a^2\frac{da}{dy} - \frac{9}{2}b\frac{db}{dy} & -a^2\frac{db}{dy} + \frac{3}{2}ab\frac{da}{dy} \\ -3a\frac{db}{dy} + \frac{9}{2}b\frac{da}{dy} & a^2\frac{da}{dy} + \frac{9}{2}b\frac{db}{dy} \end{pmatrix}.$$

Proof. An explicit calculation direct from the definition which uses the Sylvester matrix of $Q(x,y) = x^3 + a(y)x + b(y)$ and $\frac{\partial Q}{\partial x}$ with respect to x, and Kedlaya's formula for pole reduction of differential forms [15]. $\qquad\square$

Let $\bar{K}$ be an algebraic closure of K, and $R := \{\gamma \in \bar{K} \mid \Delta(\gamma) = 0\}$. Let $\mathrm{M}(K[y], 2)$ be the ring of 2×2 matrices over $K[y]$. Define $\beta(y) \in \mathrm{M}(K[y], 2)$ by $\beta(y) := \Delta(y)B(y)$.

Lemma 8.6. *The matrix $\beta(\gamma)$ is nilpotent for all $\gamma \in R$.*

Proof. First, from Proposition 8.5 observe $\mathrm{Tr}(\beta(y)) = 0$. An explicit calculation reveals that

$$\det(\beta(y)) = -\frac{1}{4}\Delta(y)\left(a\left(\frac{da}{dy}\right)^2 + 3\left(\frac{db}{dy}\right)^2\right).$$

So at a root γ of $\Delta(y) = 0$ we have $\det(\beta(\gamma)) = 0$, and hence $\det(T - \beta(\gamma)) = T^2$, as required. $\qquad\square$

Proposition 8.7. *Assume that $\Delta(y)$ is squarefree, and let $\gamma \in R$. Let $t_\gamma := y - \gamma$, a uniformizing parameter at γ, $K(\gamma)((t_\gamma))$ be the field of Laurent series, and embed $K[y, 1/\Delta(y)] \hookrightarrow K(\gamma)((t_\gamma))$. Then*

$$B(t_\gamma) = r_\gamma t_\gamma^{-1} + s_\gamma(t_\gamma), \; s_\gamma(t_\gamma) \in \mathrm{M}(K(\gamma)[[t_\gamma]], 2)$$

where the residue matrix $r_\gamma \in \mathrm{M}(K(\gamma), 2)$ is nilpotent.

Proof. We have

$$B(y) = \frac{\beta(y)}{\Delta(y)} = \frac{\beta(y)}{\Delta'(y)} \sum_{\gamma \in R} \frac{1}{y - \gamma}.$$

Let $\gamma \in R$. Then $B(t_\gamma)$ can be written as claimed where $r_\gamma := \beta(\gamma)/\Delta'(\gamma)$. Since $\beta(\gamma)$ is nilpotent, it follows that r_γ is nilpotent. $\qquad\square$

Thus under the hypothesis that $\Delta(y)$ is squarefree, the Gauss-Manin has regular singular points at the roots of $\Delta(y) = 0$, with nilpotent residue matrix. So we have proved in an entirely explicit manner the following well-known result.

Corollary 8.8. *When the discriminant $\Delta(y)$ is non-constant and squarefree, the family of elliptic curves defined by the equation $z^2 = x^3 + a(y)x + b(y)$ has regular singularities and unipotent local monodromy at the roots of $\Delta(y) = 0$.*

We now consider the local monodromy at infinity. First, let us consider the case which arises in our calculations in Section 9.

Lemma 8.9. *Assume that $\deg(a) \leq \deg(b)/2$ and $\deg(\Delta) = 2\deg(b)$. Then we have $\deg_y(B(y)) \leq -1$, and the coefficient of y in the local expansion at zero of $B(y)$ has the form*

$$\frac{1}{27} \begin{pmatrix} -\frac{9}{2}\deg(b) & \star \\ 0 & \frac{9}{2}\deg(b) \end{pmatrix}$$

where $\star = 0$ when $\deg(a) < \deg(b)/2$. When $\deg(a) = \deg(b)/2$ we have

$$\star = \frac{\alpha^2}{\beta}\left(-\deg(b) + \frac{3}{2}\deg(a)\right) = -\frac{\alpha^2}{4\beta}\deg(b),$$

where α and β are the leading coefficients of a and b, respectively.

Proof. This can be read off from the connection matrix in Proposition 8.5. $\qquad\square$

When $\deg(b) \equiv 0 \bmod 6$, as in Section 9, the residue matrix has integer eigenvalues $\pm \deg(b)/6$. Note that since the residue matrix is not prepared in this case, one cannot apply directly the precision loss bounds deduced in [18, Section 4] when reducing the "polynomial part" of differential forms. However, by virtue of our proof of [18, Conjecture 7.4], very little reduction needs to be done on the "polynomial part", and naive estimates are sufficient.

When $\deg(a) \geq \deg(b)$ and $\deg(\Delta) = 3\deg(a)$, the matrix $B(y)$ is such that $\deg_y(B(y)) \leq -1$, and one can explicitly read off the residue matrix. However, in the case $\deg(b)/2 < \deg(a) < \deg(b)$ the entry $B_{1,2}(y)$ does not have a simple pole at infinity and one needs to make a change of basis. We explain how to do this in the proof of Proposition 8.10, although we do not examine the local monodromy at infinity. Note that we have not implemented this change of basis routine in our algorithm as it requires an extension of the base field. The author does not know whether a Fuchsian basis exists for the general case without first extending the base field.

Assume $\deg(b)/2 < \deg(a) < \deg(b)$ and $d := \deg(\Delta) = \max\{2\deg(b), 3\deg(a)\} > 0$. When $\deg(a) \leq 2\deg(b)/3$ define $m := 2\deg(a) - \deg(b)$, and when $\deg(a) > 2\deg(b)/3$ define $m := \deg(b) - \deg(a)$. Note that $m + 1$ is the pole order at infinity of $B_{1,2}(y)$. Assume that $\Delta(y)$ is squarefree, and also that either $B_{1,1}(y)$ or $B_{2,1}(y)$ is non-zero.

Proposition 8.10. *Let $L \supseteq K$ be such that $\Delta(y)$ has a root $\gamma \in L$ and a factor of degree m defined over L. Then there exists a basis for $H^1_{dR}(\mathcal{V}_K/\mathcal{S}_K) \otimes_K L$ such that the matrix for the Gauss-Manin connection ∇ is Fuchsian (see Section 7.1 for the definition of this term).*

Proof. After a change of variable $y \mapsto y - \gamma$ we may assume $\gamma = 0$. We make a further change of variable $t := 1/y$. The matrix for the connection ∇ with respect to the same basis but different choice of coordinate function t is $\tilde{B}(t) := -1/t^2 B(1/t)$. Define $\tilde{\Delta} := t^d \Delta(1/t)$. Then from Proposition 8.5 one sees

$$\tilde{B}(t) = \begin{pmatrix} \frac{c(t)}{t\tilde{\Delta}(t)} & \frac{d(t)}{t^{m+1}\tilde{\Delta}(t)} \\ \frac{t^{m-1}e(t)}{\tilde{\Delta}(t)} & -\frac{c(t)}{t\tilde{\Delta}(t)} \end{pmatrix}, \text{ where } c(t), d(t), e(t) \in L[t] \text{ , } e(t) \text{ or } c(t) \text{ non-zero.}$$

Moreover, since $B(y)$ had a simple pole at $y = 0$, one sees that $\deg(c) \leq \deg(\tilde{\Delta})$, $\deg(d) \leq \deg(\tilde{\Delta}) + m$ and $\deg(e) \leq \deg(\tilde{\Delta}) - m$. Now make a change of basis using the matrix

$$H(t) := \begin{pmatrix} g(t) & \alpha(t) \\ 0 & t^m \end{pmatrix}$$

where $g(t)$ is a factor of $\tilde{\Delta}(t)$ of degree m, and $\alpha(t) \in L[t]$ will shortly be chosen. One computes that $\tilde{B}_{[H]}$ (see (18)) equals

$$\begin{pmatrix} \frac{c-\alpha e}{t\tilde{\Delta}} + \frac{g'}{g} & \frac{2c\alpha - e\alpha^2 + d}{t\tilde{\Delta}g} + \frac{\alpha'}{g} - \frac{m\alpha}{tg} \\ \frac{eg}{t\tilde{\Delta}} & \frac{e\alpha - c}{t\tilde{\Delta}} + \frac{m}{t} \end{pmatrix}.$$

Choose $\alpha \in K[t]$ with $\deg(\alpha) < \deg(g) = m$ such that

$$-e\alpha^2 + 2c\alpha + d = gf$$

for some $f \in W[t]$; that is, solve the quadratic equation $-eX^2 + 2cX + d = 0 \bmod g$. This is always possible without extending the field further: the discriminant of the equation is $4c^2 + 4ed$, which is zero modulo $\tilde{\Delta}(t)$ since the residue matrices of $\tilde{B}(t)$ are nilpotent at the roots of $\tilde{\Delta}(t)$ (by Proposition 8.7). With this choice of α one sees that the entries in the matrix $\tilde{B}_{[H]}$ are of the form $\star/t\tilde{\Delta}(t)$ where $\deg(\star) \leq \deg(\tilde{\Delta})$. $\qquad\square$

8.4 Complexity estimates

All of the complexity estimates in this section are for deterministic algorithms. Let $\bar{Q}(x, y) \in \mathbb{F}_q[x, y]$ with $\deg_x(\bar{Q}) = 2g + 1$ and $h := \deg_y(\bar{Q})$. From [19, Theorem 1] we see that one may compute the L-function of a hyperelliptic curve $z^2 = \bar{Q}(x, y)$ over $\mathbb{F}_q(y)$ in $(pgh \log(q))^C$ bit operations for some absolute constant $C \geq 1$. For g fixed and h/p bounded, [18, Theorem 8.6] tells us we may compute the L-function in $\mathcal{O}(p^{1+\varepsilon} \log(q)^{3+\varepsilon} h^{4+\varepsilon})$ bit operations, for any $\varepsilon > 0$. Let us now assume $\bar{Q}(x, y)$ satisfies the hypothesis in the statement of Theorem 8.4. For h fixed, using ideas similar to those in the last paragraph of [18, Section 8.3] and Theorem 8.4 one can show that the L-function may be computed in $\mathcal{O}(p^{1+\varepsilon} \log(q)^{3+\varepsilon} g^{7+\varepsilon})$ bit operations, for any $\varepsilon > 0$. The main point is that the bound in Theorem 8.4 does not grow with g. This last bound does not use any of the refinements in this paper other than the proof of [18, Conjecture 7.4].

Assume now that g is fixed. The difficulty lies in proving bounds when h/p is allowed to grow. The problem is that using the method in [18], even combined with our proof of [18, Conjecture 7.4], one can only show that the matrix of the pth power Frobenius on $H^2_{rig}(V)$ has valuation bounded below by some absolute constant times $-h/p$. This lower bounds impacts on the complexity when one computes the characteristic polynomial, because of the possibility of precision loss. By computing Frobenius on the basis elements of the lattice $H(X, kD)$ in Section 4.3 one gets a matrix whose valuation is bounded below by some absolute constant times $-\log_p(h)$, and so there is no problem with precision loss when one computes the characteristic polynomial. Unfortunately, as yet the author has not been able to prove useful bounds during another step of the refined algorithm; namely after reduction in the cokernel of ∇, when an element of $H(X, kD) \otimes_W K$ written w.r.t a given generating set for $H^2_{rig}(V)$ is written as a linear combination of the chosen basis for $H(X, kD)$. In practice, this does not cause any problems: this step can be accomplished by multiplication by an explicit matrix with entries in an algebraic number field, and one can measure the loss of precision simply by computing

29

the valuation of the matrix at the prime p. In the examples computed in Section 9, this loss of precision was zero; note that this precision loss can be computed right at the start of the algorithm, before various precisions are chosen. Assuming the loss of precision at this step is bounded by some function of $\log_p(h)$, then one gets a complexity of $\mathcal{O}(p^{1+\varepsilon}\log(q)^{3+\varepsilon}h^{4+\varepsilon})$, for any $\varepsilon > 0$. One must assume here that all of the conditions needed for the various steps are met. For elliptic curves with discriminant of degree $12e$ it is sufficient that $p > 3$ and p does not divide e, $Q(x,y) = x^3 + \bar{a}(y)x + \bar{b}(y)$ with $\deg(a) \leq \deg(b)/2$, the discriminant $4\bar{a}^3 + 27\bar{b}^2$ is squarefree, the affine surface $z^2 = \bar{Q}(x,y)$ is smooth, the projective surface defined by the affine equation $z^{6e} = \bar{Q}(x^{2e}, y)$ is smooth, and torsion is not encountered during the construction of the lattice $H(X, kD)$ in Section 4.3. We stress that the output of the algorithm is always provably correct.

9   Ranks of elliptic curves

For each $d \in \{6, 12, 18, 24, 30\}$, the author selected in a verifiably random manner 1000 elliptic curves of the form
$$z^2 = x^3 + a(y)x + b(y)$$
where $a, b \in \mathbb{F}_7[y]$ with $\deg(b) = d$ and $\deg(a) \leq d/2$, subject to the condition that the discriminant is squarefree and does not vanish at $y = 0$. We imposed the further condition that the projective surface defined by the affine equation $z^d = x^d + a(y)x^{d/3} + b(y)$ is smooth, see Note 9.1. The L-functions of the curves were computed using the fibration method. These are polynomials of degree $2d - 4$ with all reciprocal roots of complex absolute value 7. The curves and their L-functions, along with the details of how the curves were generated, will appear as an attachment in the final version of this paper. The table below details the number of curves of each analytic rank.

	$d = 6$	$d = 12$	$d = 18$	$d = 24$	$d = 30$
analytic rank 0	336	378	449	473	505
analytic rank 1	481	489	489	496	482
analytic rank 2	162	120	55	31	13
analytic rank 3	19	11	7	0	0
analytic rank 4	2	2	0	0	0
analytic rank > 4	0	0	0	0	0

Assuming the Tate conjecture, one observes that the percentage with infinitely many rational points is 66.4%, 62.2% (these are elliptic K3 surfaces, so the Tate conjecture is known here [24, Theorem 5.6. (b)]), 55.1%, 52.7% and 49.5%, respectively — neatly flattening from the previous experimentally observed fraction of around two thirds to around the predicted value of one half.

Note 9.1 The additional generic condition that the projective surface defined by the affine equation $z^d = x^d + a(y)x^{d/3} + b(y)$ is smooth is an artifact of the method of construction of the W-lattice $H(X, kD)$ in Section 4, and undoubtedly irrelevant to the algorithm and the correctness of its output. The table for the first 1000 curves chosen without imposing this condition is as follows.

	$d = 6$	$d = 12$	$d = 18$	$d = 24$	$d = 30$
analytic rank 0	346	379	453	479	497
analytic rank 1	471	494	493	493	493
analytic rank 2	162	114	47	28	10
analytic rank 3	20	11	7	0	0
analytic rank 4	1	2	0	0	0
analytic rank > 4	0	0	0	0	0

Assuming the Tate conjecture, one observes that the percentage with infinitely many rational points here is 65.4%, 62.1%, 54.7%, 52.1% and 50.3%, respectively.

Note 9.2 The restriction that $\deg(a) \leq d/2$, rather than the more natural $\deg(a) \leq 2d/3$, forces the j-invariants of the curves chosen to vanish to a high degree at infinity. So we have not chosen curves randomly in a dense open subset of all elliptic curves with discriminant of degree $2d$. However, the curves are chosen uniformly at random from a dense open subset of a "Weiestrass family" which for $d \geq 12$ has geometric monodromy group the full orthogonal group $O(2d-4)$ [14, Theorem 10.2.13]. What we are really testing experimentally are the predictions of Katz for such families as one allows the degree of the conductor to grow [13, Introduction]. These predictions include that asymptotically exactly one half will have infinitely many rational points.

References

[1] T.G. Abbot, K.S. Kedlaya, D. Roe, Bounding Picard numbers of surfaces using p-adic cohomology, to appear in Arithmetic, Geometry and Coding Theory (AGCT 2005), Societé Mathématique de France.

[2] B. Bektemirov, B. Mazur, W. Stein and M. Watkins, Average ranks of elliptic curves: tension between data and conjecture, Bull. A.M.S. **44**(2), (2007), 233-254.

[3] A.A. Bolibrukh, The Riemann-Hilbert problem, Russian Math. Surveys **45** (2), (1990), 1-47.

[4] D.A. Cox and S. Katz, Mirror Symmetry and Algebraic Geometry, Mathematical Surveys and Monographs **68**, A.M.S., 1999.

[5] W. Dekkers, The matrix of a connection having regular singularities on a vector bundle of rank 2 on $P^1(C)$, L.N.M. Vol. 712, 33-43, Springer, New York, 1979.

[6] P. Deligne, La conjecture de Weil: II, Pub. I.H.E.S. **52**, (1981), 313-428.

[7] A. Dimca, Singularities and coverings of weighted complete intersections, J. Reine Angew. Math. **366** (1986), 184-193.

[8] A. Dimca, Singularities and Topology of Hypersurfaces, Springer-Verlag, 1992.

[9] A. Dimca, Sheaves in Topology, Springer-Verlag, 2004.

[10] R. Gerkmann, Relative rigid cohomology and deformation of hypersurfaces, to appear in Intern. Math. Research Papers.

[11] R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics 52, Springer, 1977.

[12] N.M. Katz, Nilpotent connections and the monodromy theorem: applications of a result of Turrittin, Pub. I.H.E.S. **39**, (1970), 175-232.

[13] N.M. Katz, Twisted L-functions and Monodromy, Annals of Mathematics Studies **150**, Princeton University Press, 2002.

[14] N.M. Katz, Moments, Monodromy, and Perversity: A Diophantine Perspective, Annals of Mathematics Studies **159**, Princeton University Press, 2005.

[15] K. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, J. Ramanujan Math. Soc. **16**, (2001), 323-338.

[16] K. Kedlaya, Finiteness of rigid cohomology with coefficients, Duke Math. J. **134**, (2006), 15-97.

[17] K. Kedlaya, Search techniques for root-unitary polynomials, arxiv:math/0611835v3, to appear in Proceedings of a Special Session on Computational Arithmetic Geometry, A.M.S. (K. Lauter and K. Ribet, eds).

[18] A.G.B. Lauder, A recursive method for computing zeta functions of varieties, L.M.S. J. Comp. Math. **9**, (2006), 222-267.

[19] A.G.B. Lauder and D. Wan, Counting points on varieties over finite fields of small characteristic, in "Algorithmic Number Theory: lattices, number fields, curves and cryptography", J.P. Buhler and P. Stevenhagen (eds), MSRI Publ. **44**, to appear.

[20] B. Le Stum, Rigid cohomology, Cambridge Tracts in Mathematics 172, Cambridge University Press, 2007.

[21] B. Mazur, Frobenius and the Hodge filtration, Bull. A.M.S. **78** (5), (1972), 653-667.

[22] J. Steenbrink, Intersection form for quasi-homogeneous singularities, Compositio Mathematica **34**, (1977), 211-223.

[23] J. Tate, Algebraic cycles and poles of zeta functions, Arithmetic Algebraic Geometry, Harper and Row, New York, (1965), 93-110.

[24] J. Tate, Conjectures on algebraic cycles in ℓ-adic cohomology, Proc. Symp. Pure Math. **55** Part 1, (1994), 71-83.

[25] N. Tsuzuki, On the Gysin isomorphism in rigid cohomology, Hiroshima Math. J. **29**, (1999), 479-527.